ESSENTIALS OF E-DISCOVERY

SECOND EDITION



Essentials of E-Discovery

Second Edition



Essentials of E-Discovery

Second Edition

Judge Xavier Rodriguez Editor



Austin 2021

The State Bar of Texas, through its Texas Bar Books Department, publishes practice books prepared and edited by knowledgeable authors to give practicing lawyers and judges as much assistance as possible. The competence of the authors ensures outstanding professional products, but, of course, neither the State Bar of Texas, the editors, nor the authors make either express or implied warranties in regard to the use or freedom from error of this publication. In the use or modification of these materials, each lawyer must depend on his or her own expertise and knowledge of the law.

IRS CIRCULAR 230 NOTICE: To ensure compliance with requirements imposed by the IRS, we inform you that (1) this written material was not intended or written by the author(s) to be used for the purpose of avoiding federal penalties that may be imposed on a taxpayer; (2) this written material cannot be used by a taxpayer for the purpose of avoiding penalties that may be imposed on the taxpayer; (3) this written material cannot be used in promoting, marketing, or recommending to another party any tax-related transaction or matter; and (4) a taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor.

The use of the masculine gender in parts of this book is purely for literary convenience and should, of course, be understood to include the feminine gender as well.

It is not the policy of the State Bar of Texas to assert political positions. It is our hope that this publication fosters healthy discussion about legal issues and the legal profession. Any views expressed in this publication are those of the authors and do not necessarily reflect the opinions of the leadership or staff of the Bar.

International Standard Book Number: 978-1-938873-83-6 Library of Congress Control Number: 2021930665

> © 2014, 2021 State Bar of Texas Austin, Texas 78711

Parts of chapter 2 were included in Shira A. Scheindlin, Daniel J. Capra, and The Sedona Conference, *Electronic Discovery and Digital Evidence, Cases and Materials*, 2nd ed. (West Academic Publishing 2012) and are reprinted with permission of West Academic.

All rights reserved. Permission is hereby granted for the copying of any part of this publication by a photocopy or other similar process or by manual transcription, by or under the direction of licensed attorneys for use in the practice of law. No other use is permitted that will infringe the copyright without the express written consent of the State Bar of Texas.

Printed in the United States of America

Second Edition, 2021



Authors

ALEXANDER S. ALTMAN

Alex Altman is an associate at Norton Rose Fulbright and a 2013 graduate of Fordham University School of Law. He holds a B.A. in philosophy from Vassar College. His areas of interest include e-discovery, data privacy, and commercial litigation.

KEITH M. ANGLE

As a senior counsel in Norton Rose Fulbright's Houston office, Keith Angle assists clients with their e-discovery and information governance needs, particularly e-discovery strategy and record lifecycle issues, including data disposition processes. Keith regularly consults with his clients' IT and Records Management personnel on ediscovery and information governance matters. He is often called on to help in complex litigation discovery projects, and advises on issues from document preservation and collection to production for large national clients.

CRAIG BALL

Craig Ball hails from Texas, works in Austin, and happily calls the Big Easy home. Licensed in Texas since 1982, Craig is an adjunct professor at the University of Texas School of Law as well as the Tulane Law School, teaching courses on electronic evidence and digital discovery. Craig is an expert in digital forensics, emerging technologies, visual persuasion, electronic discovery, and trial tactics, limiting his practice to service as a court-appointed special master in electronically stored information. He has served as the special master or testifying expert in some of the most challenging and celebrated cases in the United States. Craig is a founder and faculty member of the Georgetown University Law Center E-Discovery Training Academy. Craig is also an instructor in computer forensics and electronic evidence to multiple law enforcement and security agencies. For nine years, he wrote "Ball in your Court," the award-winning column on computer forensics and e-discovery for American Lawyer Media, and still pens for **ballinyourcourt.com**. Craig speaks at CLE programs for the bench and the bar throughout the world. Craig is the 2019 recipient of the Texas Bar's Gene Cavin Award for Lifetime Achievement in Continuing Education.

KATHY OWEN BROWN

Kathy Owen Brown's practice is focused on complex litigation, including professional liability, pharmaceutical, medical device, and mass tort litigation, as well as advising national and international clients in all phases of electronic discovery and information management. She is a frequent speaker on issues relating to legal ethics, e-discovery, social media, and data privacy. Kathy's professional liability practice represents accounting firms in malpractice actions and regulatory matters before the Public Company Accounting Oversight Board and the Securities and Exchange Commission. She's had twelve years of service on the Supreme Court of Texas Board of Disciplinary Appeals. Kathy is a member of DLA Piper's North American Pro Bono Committee, which included a pro bono project to support the practicing lawyers in Kosovo by drafting ethics rules and procedures for the Kosovo bar. There, she spent time delivering training on legal ethics and consulted with local lawyers on ways to improve the country's disciplinary system and delivery methods for continuing legal education.

JUSTICE JOHN G. BROWNING

Justice John Browning has a long record of leadership and service to the bar. He served on the Fifth District Court of Appeals and has spent more than thirty-one years as a trial and appellate lawyer as a partner with large national law firms and his own small law firm. While in private practice, Justice Browning's vast experience has encompassed personal injury and wrongful death; product liability; commercial litigation; intellectual property disputes; employment matters; consumer protection and DTPA cases; professional liability; health care; class action litigation; defamation and media law; and cyberliability and data privacy. Justice Browning received bachelors degrees in History and Comparative Literature in 1986 from Rutgers University, where he was a National Merit Scholar, Phi Beta Kappa, and Henry Rutgers Scholar. He received his J.D. in 1989 from the University of Texas School of Law, where he received awards for legal writing and advocacy. A noted legal author and CLE speaker, Justice Browning has received the Bar's highest honors for legal writing, legal ethics, and public service. He is the author of five law books, more than forty law review articles, and hundreds of other articles on legal subjects.

STEPHEN A. CALHOUN

Stephen A. Calhoun is a litigation partner in the San Antonio, Texas, office of Jackson Walker L.L.P. Stephen represents companies from a variety of industries as both plaintiffs and defendants in state and federal courts throughout Texas and across the country. Stephen focuses on complex commercial disputes, including contract

claims and real estate disputes. He also represents clients in responding to governmental investigations related to health care and other highly regulated industries. Stephen earned a B.A. from the University of Virginia and a J.D. from the University of Texas School of Law. Following law school, Stephen served as a law clerk for Judge Douglas H. Ginsburg on the U.S. Court of Appeals for the D.C. Circuit.

EMMA CANO

Emma Cano is a founding member of Jefferson Cano, a litigation firm focusing primarily on complex commercial disputes, with experience litigating matters in both federal and state courts. Before Jefferson Cano, Emma worked her way up to partner at a large international law firm with offices in San Antonio. Her cases cover a range of commercial issues, including fraud, partnership disputes, franchise-related controversies, contract and construction disputes, bond claims, and insurance coverage disputes. Emma has defended numerous catastrophic injury and fatality claims in a variety of industries and has represented businesses in tort matters. Additionally, Emma represents companies involved in OSHA investigations.

CHRISTOPHER C. COSTELLO

Christopher C. Costello is a senior e-discovery attorney in Winston & Strawn's eDiscovery & Information Governance Practice Group. He concentrates his practice on e-discovery, privacy and data security, and international and cross-border discovery issues. He regularly advises clients on dealing with General Data Protection Regulation and its requirements for obtaining information for use in U.S. litigations and how clients can adequately prepare for and standardize their approach to these requests. Chris also counsels clients on information governance, including legacy retirement, records retention, litigation readiness programs, and bring-your-own-device programs, as well as general data privacy issues and cost-effective approaches to e-discovery. He has successfully defended against spoliation and sanctions claims and works to educate attorneys and judges on the intricacies of international data privacy and cross-border discovery. Chris is a Certified Information Privacy Professional and a member of the International Association of Privacy Professionals. He is a frequent speaker on cross-border discovery, data privacy, and general e-discovery issues.

JUDGE KARL E. HAYS

Associate District Judge Karl E. Hays is the presiding judge of the family court of Hays County, Texas, where he is routinely called on to address issues regarding electronically stored information. Before his appointment in 2019, Karl was a solo practitioner who practiced throughout central Texas. He is board certified in civil trial law, civil appellate law, and family law by the Texas Board of Legal Specialization. He is a 1985 graduate of St. Mary's University School of Law. Karl is a fellow at the American Academy of Matrimonial Lawyers, a member of the Texas Academy of Family Law Specialists, a member of the Texas Family Law Foundation, and he is currently serving on the family law council to the Family Law Section of the State Bar of Texas. Karl is a frequent speaker on issues relating to the practice of family law.

JUDGE DAVID L. HORAN

United States Magistrate Judge David L. Horan took the bench in the Dallas division of the Northern District of Texas on November 21, 2012. Before his swearing in, David was a partner in the Dallas office of Jones Day where he led the firm's Issues and Appeals Practice Group in its Texas offices. Before joining Jones Day in 2004, David was an associate with Hughes & Luce, LLP, in Dallas. He received a B.A. in government and philosophy from the University of Notre Dame in 1996 and a J.D. from Yale Law School in 2000. Upon graduation, he served as law clerk to United States District Judge Janet C. Hall in Bridgeport, Connecticut, from 2000 to 2001, and as law clerk to United States Court of Appeals Judge Patrick E. Higginbotham in Dallas from 2001 to 2002.

MAX KELLOGG

Max Kellogg joined Norton Rose Fulbright in 2018. His practice focuses on commercial litigation, e-discovery, cybersecurity, and data privacy matters. His experience includes assisting clients on contract disputes and internal investigations, as well as assisting clients with a range of discovery issues, including second requests under the Hart-Scott-Rodino Act and subpoena responses. He counsels clients with issues surrounding compliance with data privacy laws, incident response, and data breach notification laws and obligations. He has been the author or coauthor of numerous articles, including for the *New York Law Journal*. Max earned a J.D. from the Emory University School of Law in 2018.

DAVID J. KESSLER

David J. Kessler is a partner in the New York office of Norton Rose Fulbright and is the head of its Data and Information Risk Practice. David focuses his practice on e-discovery, privacy, information governance, and cybersecurity. He advises clients on strategic and tactical questions regarding data management, e-discovery, and, in particular, on cross-border privacy, discovery, and cyber security. David teaches e-discovery as an adjunct professor at the University of Pennsylvania Law School. Among his professional honors, David is ranked in the top six e-discovery lawyers in the United States by Chambers & Partners, and was recently elected as a member of the American Law Institute.

SUMERA KHAN

Sumera Khan is a partner in the Norton Rose Fulbright Houston office where her practice focuses on e-discovery and information governance, data privacy, and commercial litigation. She has counseled clients in the energy, health care, insurance, and pharmaceutical industries on issues arising from litigation as well as requests for compliance advice. Sumera assists clients in navigating complex electronic discovery issues and has provided clients across all industries with advice on litigation readiness and cross-border discovery issues. Sumera has also served as special discovery counsel to clients in multi-district and complex litigation matters and has provided clients with representation in managing document discovery for large government investigations as well.

RAMONA L. LAMPLEY

Ramona L. Lampley is the associate dean for academic affairs at St. Mary's University School of Law in San Antonio. She teaches civil procedure, complex litigation, e-discovery, sales, secured transactions, and commercial paper. Ramona's scholarship is in litigation, dispute resolution, and consumer contracts. She has been published in American University Law Review, Washington Law Review, BYU Law Review, and Cornells Journal of Law and Public Policy, and is coauthor of Texas Practice: Consumer Rights & Remedies and The Consumer Law Handbooks. Ramona frequently comments on arbitration and consumer law issues for the San Antonio Express News. Ramona is chair of the Article 2 subcommittee of the U.C.C. committee for the ABA's Business Law Section and is a member of the Working Group for Implementation of Human Rights Protections in Supply Side Contracts. She graduated from the Wake Forest University School of Law in 2004 and then clerked for the Honorable Harris L. Hartz on the United States Circuit Court for the Tenth Circuit. Before joining the faculty at St. Mary's School of Law, Ramona practiced civil litigation at Wheeler Trigg O'Donnell LLP in Denver, Colorado, where she handled a variety of cases involving commercial contract disputes, class actions, and professional malpractice. She was recognized as one of Denver's "40 Under 40" rising professionals in 2012, and as one of Colorado Super Lawyer's Rising Stars in 2012.

JONATHAN LASS

Jonathan Lass is a partner at Jackson Walker where he represents both the private sector and government clients on mission-critical technology outsourcing and merger and acquisition transactions. Jonathan's recent engagements include efforts on behalf of the University of Texas, Texas Department of Transportation, Texas Office of Court Administration, and the Texas Secretary of State. Along with his practice, Jonathan invests substantial time teaching and mentoring law students at his alma mater, the University of Texas School of Law, including a course on negotiation, which he has taught since 2017.

PAUL M. LEOPOLD

Paul Leopold is an associate at KoonsFuller Family Law and focuses his practice on family law appeals. Paul joined KoonsFuller in 2015 after clerking for the Eastland court of appeals. Paul primarily acts as appellate counsel on cases such as complex property disputes, custody or child support, international child abduction, and constitutional rights of parents. As appellate counsel, Paul assists trial attorneys with strategy, research, briefing, discovery, dispositive motions, and trial or settlement. He also prosecutes and defends appeals and original proceedings in the Supreme Court of Texas, the Texas Courts of Appeals, and the United States Courts of Appeals.

JULIA W. MANN

Julia W. Mann serves as the managing partner of Jackson Walker's San Antonio office. An experienced litigator, Julia represents clients on both sides of the docket and has appeared in matters in more than forty counties across Texas and Oklahoma. Her practice encompasses contractual disputes, professional liability claims, actions to protect companies' proprietary information, and business torts such as fraud, negligent misrepresentation, breach of fiduciary duty, and tortious interference. She represents leading Texas industries in the energy, agriculture, and banking sectors and is known for her fiduciary litigation work. Before becoming office managing partner in 2019, Julia served as chair of the Trial and Advocacy Section for her San Antonio office and the statewide chair for Litigation Attorney Development and Training. Julia has served as an author and speaker on the subject of e-discovery, particularly on issues of cost shifting and rule 30(b)(6) depositions. In recognition of her work, Julia has been among "The Best Lawyers in America" in the area of commercial litigation since 2018, was named to Thomson Reuters' "Super Lawyers" from 2012 to 2019, and named to "Top Women Attorneys in Texas" in 2020. She received a J.D. in 1994 from St. Mary's University School of Law and a B.A. from the University of Texas in 1991.

ERIC J. MAYER

Eric J. Mayer has litigated complex commercial matters at Susman Godfrey for twenty-five years. He has represented both plaintiffs and defendants in state and federal courts across the country. Eric is a frequent speaker and author on e-discovery issues.

HEATHER MCFARLANE

Heather McFarlane began her career as a litigator at one of Houston's largest law firms, representing Fortune 500 companies in matters involving voluminous documents, including e-mails. In 2010 she formed her own firm where she continued to help her clients and colleagues formulate common-sense, efficient, and cost-effective approaches to e-discovery. Heather's mantra for e-discovery (and other aspects of litigation) is "cooperate!" Heather is a full-time mediator, focusing on solutions to conflict. She graduated from the University of Texas School of Law in 1998. She is a member of the ABA Alternative Dispute Resolution section and the Association of Attorney-Mediators. Heather was recently elected treasurer to the Houston Bar Association's ADR section.

LAWRENCE MORALES II

Lawrence Morales II is certified by the Texas Board of Legal Specialization as a labor and employment law specialist and has successfully represented individuals and companies in complex employment law and business litigation matters. After graduating from Baylor Law School, Lawrence served as a law clerk to the Honorable Priscilla R. Owen of the United States Fifth Circuit Court of Appeals. Lawrence is a frequent author and speaker on employment law and litigation topics, and he has been published in *Texas Bar Journal, The Advocate*, and *San Antonio Lawyer*. Lawrence lives in San Antonio.

ERIC J. R. NICHOLS

Eric J. R. Nichols practices both criminal and civil trial law as a partner with the Butler Snow firm based out of the firm's Austin office. Eric has been in both government and private practice during his thirty-year legal career. His most recent government practice assignment was as Deputy Attorney General for Criminal Justice for the Office of the Texas Attorney General. While overseeing the attorney general's criminal justice divisions, he remained actively engaged in trial and appellate practice. Eric also previously served as an Assistant United States Attorney for the Southern District of Texas, where he prosecuted white-collar federal criminal matters, including fraud cases relating to health care, banking, investments, customs enforcement, bankruptcy, tax matters, and government procurement. Eric is board certified in criminal law by the Texas Board of Legal Specialization. He obtained a J.D. in 1989 from the University of Texas School of Law where he served as editor-in-chief of *Texas Law Review*. Eric's work for clients in civil and criminal cases has been profiled in and on, among other places, *60 Minutes*, CNN, A&E, truTV, *National Law Journal*, *Texas Monthly*, *Texas Lawyer*, and daily newspapers across the country.

STEPHEN ORSINGER

Stephen Orsinger has been named a Texas Super Lawyer Rising Star (2010, 2011, and 2012). He is a frequent speaker on family law and e-discovery issues. A graduate of St. John's College and the University of Texas School of Law, he is a member of the Bill Review Committee of the Texas Family Law Foundation.

DAN REGARD

Dan Regard is an e-discovery and computer science consultant with twenty-five years' experience consulting legal and corporate entities. A programmer and an attorney by training, Dan has conducted system investigations, created data collections, and managed discovery on more than a thousand matters. He is responsible for the development and implementation of case and matter strategies that leverage technology in litigation and investigations. He has both national and international experience advising on such issues as e-discovery, computer forensics, structured data, and information management. He is a frequent speaker, teacher, and publisher on e-discovery issues. Dan is a member of the Sedona Conference Working Group 1: Electronic Document Retention and Production, and Working Group 6: International Electronic Information Management, Discovery and Disclosure. He is a board member of the Georgetown Advanced Institute for e-Discovery, is one of the original four founders of the E- Discovery Institute, and is a founding member of the Masters Cabinet. Dan is also the founder of b-Discovery, a monthly e-discovery networking group.

JUDGE XAVIER RODRIGUEZ

Judge Xavier Rodriguez is a former Texas Supreme Court Justice and currently sits on the bench as a United States District Judge for the Western District of Texas. Born in San Antonio, he received a bachelor's degree from Harvard University, a master's degree from the University of Texas LBJ School of Public Affairs, and a J.D. from the University of Texas School of Law. Before assuming the bench, he was a

partner in the international law firm Fulbright & Jaworski (now known as Norton Rose Fulbright). Judge Rodriguez is a frequent speaker on continuing legal education seminars and has authored numerous articles regarding employment law, discovery, and arbitration issues, and he was the editor of the 2014 edition of Essentials of E-Discovery. He is a member of The Sedona Conference Judicial Advisory Board and the Georgetown Advanced E-Discovery Institute Advisory Board, and he serves as the Distinguished Visiting Jurist-in-Residence and adjunct professor of law at St. Mary's University School of Law. He was elected to membership in the American Law Institute and is a fellow of the American Bar Foundation and the Texas Bar Foundation. In 2011, he was awarded the Rosewood Gavel Award for outstanding judicial service from St. Mary's University School of Law. In 2017, he received the State Bar of Texas Gene Cavin Award for Excellence in CLE, recognizing his longterm contributions to continuing legal education. He is a past chair of the State Bar of Texas Continuing Legal Education Committee and the State Bar of Texas Litigation Section. He is currently enrolled in the Duke University Bolch Judicial Institute's LLM Program in Judicial Studies.

JOHN J. ROSENTHAL

John J. Rosenthal's practice involves counseling clients on a variety of trade regulation, trademark, and commercial issues. He also acts as national e-discovery counsel for numerous corporations. John is a former steering committee member of Working Group 1 of the Sedona Conference on Best Practices for Electronic Discovery and Records Management, which focuses on the development of the law regarding electronic discovery and retention issues. He is also a participant in Working Group 6 of the Sedona Conference International Electronic Information Management, Discovery and Disclosure, which focuses on international issues relating to disclosure, cross-border discovery, and privacy. John received a B.A. in political science from Johns Hopkins University in 1985 and a J.D. in 1988 from the University of Virginia School of Law. John writes and lectures extensively in the fields of e-discovery, privacy, and data breach, and is the editor-in-chief of the Electronic Discovery Institute's *Journal of eDiscovery, Privacy, Data Security and Governance.*

SUE ROSS

Sue Ross is senior counsel of Norton Rose Fulbright and is located in its New York office. Sue handles a variety of U.S. privacy matters, including security breach laws, the Electronic Communications Privacy Act, Gramm-Leach-Bliley, and HIPAA, and she assists clients with EU Safe Harbor applications. She has extensive experi-

ence with technology agreements, ranging from outsourcing to website terms and conditions to cloud and security services.

ALLISON O. SKINNER

Allison O. Skinner is Deputy General Counsel at Cadence Bank, N.A., in Birmingham, Alabama. Prior to joining the bank, Allison established her own alternative dispute resolution firm after almost two decades of representing domestic and international clients in complex litigation. Allison has served as an adjunct professor at the University of Alabama School of Law and as a visiting professor at the Thomas Goode Jones School of Law teaching e-discovery. Allison wrote the *Teacher's Manual* to the West casebook on e-discovery. Allison pioneered the use of "e-neutrals" for ediscovery disputes and is a cofounder of the American College of e-Neutrals. Allison has lectured and written extensively in the areas of e-discovery and alternative dispute resolution. She received a J.D. from the University of Alabama School of Law and a B.A. from the University of Alabama.

MATTHEW J. SWANTNER

Matthew J. Swantner is a litigation associate at Jackson Walker L.L.P. and is licensed to practice law in Texas and New Mexico. Matthew earned a B.B.A. from the University of Texas and a J.D. from the University of Texas School of Law.

PETER S. VOGEL

Peter S. Vogel is of counsel in the trial section of Foley & Lardner LLP where he chairs the eDiscovery Group. Before practicing law, he worked as a computer programmer, received a master's degree in computer science, and taught graduate courses on information systems. Peter has had trials around the U.S. on failed software implementations, intellectual property suits (including trade secrets, copyright, patent, and trademarks), and e-commerce disputes. In 1990 Peter was the founding chair of the Computer & Technology Section of the State Bar of Texas. He is a cofounder of the American College of e-Neutrals for which he conducted e-discovery training around the U.S., including the American Arbitration Association. For twelve years he's served as the founding chair of the Texas Supreme Court Judicial Committee on Information Technology, which is responsible for helping automate the Texas court system and establishing the e-filing system. Peter has taught courses at the SMU Dedman School of Law for more than thirty years, including courses on e-discovery and the law of e-commerce. Many of Peter's topics are discussed on his "Internet, IT & eDiscovery" blog (www.vogelitlawblog.com) and in his monthly legal column for E-Commerce Times (www.ecommercetimes.com).



STATE BAR OF TEXAS

2020-2021

LARRY P. MCDOUGAL, President JOHN CHARLES "CHARLIE" GINN, Chair of the Board REBEKAH STEELY BROOKER, Chair, Professional Development Subcommittee SCOTT ROTHENBERG, Chair, Committee on Continuing Legal Education TREY APFFEL, Executive Director



SHARON SANDLE, Director JILL HOEFLING, Assistant Director ELMA E. GARCIA, Senior Publications Attorney SARAH F. HENSON, Project Publications Attorney COURTNEY H. GIESINGER, Publications Attorney SUSANNAH R. MILLS, Publications Attorney JAMES W. NORMAN, Publications Attorney MICHAEL AMBROSE, Senior Editor COURTNEY CAVALIERE, Editor THOMAS OSTMEYER, Editor ROGER SIEBERT, Editor TRAVIS RIDDLE, Production Supervisor JENNIFER TOWNSEND, Production and Editorial Assistant CYNTHIA DAY, Meeting Coordinator LARA TALKINGTON, Marketing Coordinator CONOR JENSEN, Website Manager JENNIFER KARLSSON, Web Content Specialist JENNIFER PEREZ, Web Content Specialist A'NAIYA DAVIS, Web Content Strategist

Contents

Foreword	xxi
Preface	xxiii
Chapter 1	Duty to Preserve
Chapter 2	Litigation Holds
Chapter 3	Computer Usage Policies, Records Management, and Information Governance
Chapter 4	Introduction to Digital Data, Computers, and Storage Media 43 <i>Craig Ball</i>
Chapter 5	E-Mail 101
Chapter 6	Rule 26(f) Meet and Confer. 107 Ramona L. Lampley
Chapter 7	ESI Collection
Chapter 8	ESI Culling, Searching, and Reviewing
Chapter 9	Format of Production
Chapter 10	Predictive Coding and Computer-Assisted Document Review 201 Eric J. Mayer
Chapter 11	Processing in E-Discovery, a Primer
Chapter 12	Privilege Waiver, Rule 502, and Clawback/Sneak Peek Agreements

Contents

Chapter 13	Responding to Discovery Requests and Discovery Disputes Judge David L. Horan	269	
Chapter 14	Cost Shifting and 28 U.S.C. § 1920 Julia W. Mann and Judge Xavier Rodriguez	315	
Chapter 15	Spoliation and Sanctions Judge Xavier Rodriguez	339	
Chapter 16	Rule 30(b)(6) Depositions Julia W. Mann, Matthew J. Swantner, and Stephen A. Calhoun	365	
Chapter 17	Mediation of E-Discovery Disputes and Special Masters Peter S. Vogel and Allison O. Skinner	389	
Chapter 18	Authentication and Admissibility Judge Karl E. Hays and Paul M. Leopold	407	
Chapter 19	Ethical Issues in E-Discovery Kathy Owen Brown	463	
Chapter 20	Social Media Justice John G. Browning	493	
Chapter 21	Discovery of ESI from Nonparties	513	
Chapter 22	Introduction to Computer Forensics	533	
Chapter 23	Cross-Border Production Issues Christopher C. Costello and John J. Rosenthal	567	
Chapter 24	Privacy Issues David J. Kessler, Sue Ross, and Max Kellogg	613	
Chapter 25	ESI Discovery in Texas Criminal Practice Eric J. R. Nichols	635	
Chapter 26	Mobile Devices Dan Regard	673	
Appendix A: Judicial Resources			
Appendix B: Select Federal Rules of Civil Procedure			

Contents

Appendix C: Select Texas Rules of Civil Procedure	773
Appendix D: Updates to Texas Rules of Civil Procedure	795
Statutes and Rules Cited	813
Cases Cited	819
Subject Index	835
How to Download This Book	851



Foreword

I magine how our lives have changed in just one generation. Few students graduating from law school now have any memory of life before personal computers, smart phones, e-mail, text messaging, streaming music and video, or online legal research. On the other hand, few lawyers who graduated from law school before 1984 had to deal with information technology more sophisticated than an electric typewriter or fax machine before they were called to the bar.

The impact of digital information technology on the legal profession is small compared to its impact on business, government, and individuals—the lawyer's clients. The issues these clients bring to their lawyers are now entirely infused with information technology. While we have come to expect that all large enterprises rely on computer systems and the data these systems generate and store, it has only been in the past few years that we have come to realize that digital information technology touches every aspect of our lives. From the corporate merger to the common divorce, from the complex securities fraud action to the speeding ticket, nearly every case brought to today's law office will involve some electronically stored information, or "ESI"—the catch-all term designed by the framers of our rules of civil procedure to include all forms of digital information.

The explosion of ESI and our nearly complete dependence on it presents the lawyer with a paradox. On the one hand, there is potentially far more relevant recorded evidence in every case. Not only are we creating records where none existed before (such as text messages or Internet log files), but also these records are replicated on numerous devices and storage media and are very difficult to destroy. On the other hand, the sheer volume of discoverable ESI, together with its dispersion and technical complexity, requires that the lawyer approach the collection, review, request, and presentation of ESI with much more sophistication and judgment than was required of paper evidence.

Part of this new level of sophistication is a realization that in contested matters the lawyers on both sides must cooperate in the discovery process to a much higher degree than they were trained for or accustomed to in the twentieth century. Without compromising their clients' legal positions, lawyers on both sides must work together to provide the court with the factual evidence needed to render a just determination, or, in the majority of cases, for both sides to reach a just settlement of their differences. Today's lawyer needs to know how the client and opposing party create, use, and store ESI; how to identify ESI relevant to the disputed factual issues in the case; how to most efficiently preserve, collect, and review that ESI; and how to authenticate and present that evidence before the trier of fact. Both the federal and Texas rules implicitly recognize that this requires cooperation, but it is up to each individual practitioner to make this work.

Foreword

I commend the Honorable Xavier Rodriguez for undertaking to assemble in one volume these *Essentials of E-Discovery*, based on his own experience as a judge in federal court and the experience of leading Texas practitioners. I suspect that this project was motivated in no small measure by self-interest. The more sophisticated the lawyers who appear in court are, regarding e-discovery, the easier the judge's job. But I also hope that the practitioners who study this volume will benefit the civil and criminal justice systems as a whole by gathering and presenting the facts that their clients need for a just determination of their legal rights—at a cost they can afford.

Ken Withers Deputy Executive Director The Sedona Conference

Preface

The various chapters of this book have been compiled to serve as a desktop reference for attorneys practicing in Texas state courts and federal district courts located in Texas. In addition, this book should be of assistance to in-house counsel as they struggle to understand their company's preservation obligations and adopt appropriate information governance protocols.

I would like to acknowledge and thank the authors of the various chapters in this book. The individuals who have contributed to this book have done so solely in their individual capacities and not on behalf of a law firm, a court, or the State Bar of Texas.

The legal issues surrounding e-discovery are evolving. Some of the principles are well settled; many others are not. In addition, changes in technology and concerns over privacy rights make this area one that requires continuing study. The editor and the authors of this book are not providing legal advice, and attorneys should conduct their own independent research in addressing any ESI issues they may encounter.

Select portions of the Federal Rules of Civil Procedure are attached as an appendix to this book. We have provided the most current version of the proposed December 1, 2015, amendments. The reader should be aware, however, that these amendments are subject to further changes.

Finally, given the evolving nature of e-discovery, it is likely that future editions of this book will be published. If you are aware of any revisions or corrections that should be made to this edition, or if you wish to contribute any new or supplemental material for any future edition, I would appreciate the assistance.

Judge Xavier Rodriguez Editor



Essentials of E-Discovery

Second Edition



Chapter 1

Duty to Preserve

Judge Xavier Rodriguez

§ 1.1 Introduction

Electronically stored information ("ESI"), like documents and tangible things, must be preserved pursuant to state and federal regulations, state and federal case law, and internal document retention policies, if any. If a person or entity is subject to almost any type of audit, such as a bank audit or Equal Employment Opportunity Commission or Department of Labor review, ESI should be preserved. Finally, ESI—along with documents and tangible things—must be preserved when a party knows they are relevant to litigation, or should know the evidence may be relevant to future litigation. Breaching this duty to preserve ESI can result in a variety of sanctions, from monetary damages to adverse jury instructions to complete dismissal of a lawsuit in favor of the nonbreaching party. See chapter 13 of this book.

Parties or potential parties must take various steps that are paramount to avoiding sanctions. This chapter will concentrate on identifying the point at which the duty to preserve ESI attaches and describing the duty to preserve to all relevant ESI custodians.

§ 1.2 Possession, Custody, or Control (PCC)

"Possession, custody, or control of an item means that the person either has physical possession of the item or has a right to possession of the item that is equal or superior to the person who has physical possession of the item." Tex. R. Civ. P. 192.7.¹ PCC is the subject of some debate lately, specifically how to define "control." Some federal district courts in the Fifth Circuit have stated: "Rule 34's definition of possession, custody, or control, includes more than actual possession or control of [documents]; it also contemplates a party's legal right or practical ability to obtain [documents] from a [non-party] to the action."² In applying the "legal right" test, the Seventh Circuit has

^{1.} In re Methodist Primary Care Group, 553 S.W.3d 709, 722 (Tex. App.—Houston [14th Dist.] 2018, no pet.).

concluded that a defendant employer had control over Salesforce data in a wage and hour case.³

§ 1.3 Statutory and Regulatory Duties

Texas law requires that business records be kept no less than three years, unless another statutory or regulatory retention period applies. *See* Tex. Bus. & Com. Code § 72.002. Retention of a reproduction of an original record will satisfy state law retention requirements. Tex. Bus. & Com. Code § 72.003. A number of state and federal statutes and regulations require that certain documents be kept for specific minimum periods of time. For example, the Occupational Safety and Health Act requires retention of testing records, medical records, and environmental records for periods between twenty and forty years. Notwithstanding requirements in each state where an entity does business, federal laws such as the Employee Retirement Income Security Act, labor laws, and the Foreign Corrupt Practices Act establish certain retention periods and the types of records to be retained.

§ 1.4 Record Retention Policies

Many entities voluntarily implement document retention and destruction policies to internally establish a protocol for how long certain types of records will be kept. Such policies help ensure compliance with statutory and regulatory obligations and may assist a party in later litigation. In addition, although the cost of maintaining data on servers or in the cloud has decreased dramatically, these record retention policies

^{2.} See, e.g., Edwards v. 4JLJ, LLC, No. 2:15-CV-299, 2018 WL 2981154 (S.D. Tex. June 14, 2018) (4JLJ had installed in its vehicles a GPS system licensed from FleetMatics. The court concluded that control is broadly construed and includes legal right or practical ability to obtain the information, and control is shown if the resisting party has a relationship with a nonparty that supports the resisting party's ability to obtain the document.); United States v. Trinity Industries, Inc., No. 2:12-CV-89, 2014 WL 12603247, at *1 (E.D. Tex. July 1, 2014) ("right, authority, or 'practical ability' to control" documents imposes duty to preserve those documents); Duarte v. St. Paul Fire & Marine Insurance Co., No. EP-14-CV-305-KC, 2015 WL 7709433, at *5 (W.D. Tex. Sept. 25, 2015). See also In re Correra, 589 B.R. 76 (Bankr. N.D. Tex. 2018) (documents are considered to be under a party's control if the party has the practical ability to obtain the documents from another, irrespective of his legal entitlement). But see Lifesize, Inc. v. Chimene, No. A-16-CV-1109-RP-ML, 2017 WL 2999426, at *2 n.3 (W.D. Tex. June 2, 2017) ("Lifesize has not shown that as an employee Chimene has authority over Logitech such that he is able to command release of certain documents."). The Fifth Circuit to date has not provided recent specific guidance as to whether the "legal right" test must be established or whether "practical ability" suffices. In 2016, the Sedona Conference circulated a paper discussing this issue and proposed that the correct analysis is actual possession or legal right.

^{3.} Williams v. Angie's List, Inc., No. 1:16-CV-00878-WTL-MJD, 2017 WL 1318419, at *1 (S.D. Ind. Apr. 10, 2017).

Duty to Preserve

assist in purging obsolete or trivial data that unnecessarily increases the cost of reviewing and producing data in litigation. See chapter 3 of this book. In the event that data is destroyed pursuant to a reasonable policy established prior to the anticipation of litigation, courts are less likely to draw an adverse inference from such destruction of documents that otherwise would have been expected to be produced. See chapter 14.

§ 1.5 When Is Duty to Preserve Data "Triggered" in Civil Litigation?

The Federal Rules of Civil Procedure do not specify what "triggers" the duty to preserve data. Neither do most state rules formally specify the conditions that "trigger" preservation obligations. Rather, the basis of the duty to preserve was developed in the common law. *See, e.g., United States v. Shaffer Equipment Co.*, 11 F.3d 450, 462 (4th Cir. 1993) (recognizing "that when a party deceives a court or abuses the process at a level that is utterly inconsistent with the orderly administration of justice or undermines the integrity of the process, the court has the inherent power to dismiss the action"). "The policy underlying this inherent power of the courts is the need to preserve the integrity of the judicial process in order to retain confidence that the process works to uncover the truth." *Silvestri v. General Motors Corp.*, 271 F.3d 583, 590 (4th Cir. 2001). *See also Ashton v. Knight Transportation, Inc.*, 772 F. Supp. 2d 772, 800 (N.D. Tex. 2011) (citing *Victor Stanley v. Creative Pipe, Inc.*, 269 F.R.D. 497, 525–26 (D. Md. 2010) ("The duty to preserve is owed to the court, not to the party's potential adversary").

§ 1.5:1 Trigger Date—Federal Courts

Generally, federal courts have stated that the "obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003). *See also Guzman v. Jones*, 804 F.3d 707, 713 (5th Cir. 2015) (citing *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598, 612 (S.D. Tex. 2010)). The duty extends to individuals likely to have discoverable information that the disclosing party may use to support its claims or defenses. *Rimkus*, 688 F. Supp. 2d at 612–13.

§ 1.5:2 Trigger Date—Texas Courts

A party has a common-law duty to preserve evidence when it knows or reasonably should know that (1) there is a substantial chance that a claim will be filed and (2) evidence in its possession or control will be material and relevant to that claim. *Brookshire Bros. v. Aldridge*, 438 S.W.3d 9 (Tex. 2014). The Texas Supreme Court explained that a substantial chance of litigation arises when "litigation is more than merely an abstract possibility or unwarranted fear." *Brookshire Bros.*, 438 S.W.3d at 20 (citing *National Tank Co. v. Brotherton*, 851 S.W.2d 193, 204 (Tex. 1993)). *See also In re Advanced Powder Solutions, Inc.*, 496 S.W.3d 838 (Tex. App.—Houston [1st Dist.] 2016, no pet.) ("When a reasonable person would conclude from the severity of an accident or other circumstances that a substantial chance of litigation exists, a duty to preserve evidence arises.").

Applying these principles to the facts in the case, the court in In re J.H. Walker, Inc., No. 05-14-01497-CV, 2016 WL 819592 (Tex. App.-Dallas Jan. 15, 2016, no pet.) concluded that a trucking company had a duty to preserve the tractor because of the severity of the crash. In contrast, the court in In re Xterra Construction, LLC, No. 10-16-420-CV, 2019 WL 2147847 (Tex. App.-Waco May 15, 2019, no pet. h.) determined that the sole tenant of a warehouse did not have a duty to preserve after a fire because the tenant did not know that a claim would be filed against it by the landlord until the landlord e-mailed the tenant a month after the fire occurred. Likewise, in Sanders Oil & Gas, Ltd. v. Big Lake Kay Construction, Inc., 554 S.W.3d 79 (Tex. App.—El Paso 2018, no pet.), the court found that the validity of various invoices was never questioned until after the legal proceedings commenced and accordingly no duty to preserve "field notes" was triggered earlier. See also Shamoun & Norman, LLP v. Hill, 483 S.W.3d 767 (Tex. App.-Dallas 2016), rev'd on other grounds, 544 S.W.3d 724 (Tex. 2017) (law firm had no duty to preserve e-mails and texts because substantial chance for litigation did not exist before fee dispute was reasonably foreseeable).

Even when the duty to preserve evidence is triggered, however, it is not so encompassing as to require a litigant to keep or retain every document in its possession. *Trevino v. Ortega*, 969 S.W.2d 950, 957 (Tex. 1998) (Baker, J., concurring). The duty to preserve, nonetheless, does require a party to preserve what it knows or what it reasonably should know is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, or is the subject of a pending discovery sanction. *Trevino*, 969 S.W.2d at 957. These principles appear straightforward; however, applying them to specific fact patterns has generated numerous opinions.

§ 1.5:3 Likely Trigger Dates

Plaintiff's Preservation Obligations: In many cases, the duty to preserve will arise first for the plaintiff to the extent that the party filing suit knows when he contemplates initiating litigation. *See, e.g., Marten Transportation, Ltd. v. Plattform Advertising, Inc.*, No. 14-cv-02464, 2016 WL 492743, at *5 (D. Kan. Feb. 8, 2016).

Notice That Lawsuit Has Been Filed: In most cases, the duty to preserve is triggered upon notice that a lawsuit has been filed and the party is aware of the allegations asserted therein. *See Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244 F.R.D. 614 (D. Colo. 2007).

Notice That Administrative Proceeding Has Commenced: In many instances, once a party has become aware that an administrative proceeding has commenced against it, a duty to preserve relevant documents can be triggered. *See Flores v. AT&T Corp.*, No. EP-17-CV-00318-DB, 2018 WL 6588586, at *4 (W.D. Tex. Nov. 8, 2018) (duty to preserve relevant information triggered upon receiving notification of plain-tiff's charge of discrimination with EEOC).

Notice from Opposing Counsel: The obligation to preserve evidence may arise even earlier if a party has notice that future litigation is likely. If a party receives notice from opposing counsel that should cause the party to conclude that litigation is "reasonably anticipated," this likely will trigger preservation obligations. The scope of those preservation obligations, however, may be subject to dispute.

Counsel sending notices to opposing counsel, however, should be aware that at least one court has concluded that mere attempts to resolve a difference between parties does not trigger a duty to preserve evidence, unless the communication threatens litigation or includes a demand to preserve evidence. *See Cache La Poudre Feeds, LLC*, 244 F.R.D. at 621 ("While a party should not be permitted to destroy potential evidence after receiving unequivocal notice of impending litigation, the duty to preserve relevant documents should require more than a mere possibility of litigation."). In addition, "generic" demand letters to preserve that fail to provide any detail may not suffice. *See Green v. Harris County, Texas*, No. CV H-16-893, 2019 WL 2617429, at *6 (S.D. Tex. June 26, 2019) (generic preservation letter did not place Harris County officials on notice to preserve ancillary video that might have incidentally captured events preceding decedent's death). **Notice of Criminal Act or Investigation:** Being on notice of a criminal investigation or prosecution does not necessarily mean a civil action is reasonably foreseeable. While a duty to preserve exists as to the criminal matter, the duty to preserve evidence for a civil suit does not arise until the party has notice that a civil action may be filed. *See Doe v. Northside I.S.D.*, 884 F. Supp. 2d 485, 489 (W.D. Tex. 2012) (A school district's duty to preserve certain e-mails and surveillance video of a teacher's conduct with students arose no earlier than when the plaintiff's counsel sent a letter to the school district requesting that various documents be preserved, even though the teacher earlier confessed to an inappropriate relationship with a student. When the teacher admitted to the wrongdoing, the school district was on notice that criminal prosecution would result, but it took approximately another week for the district to become aware that a civil suit might be filed, at which time the duty to preserve attached.).

Factors to Consider in Analysis of Whether Litigation Is or Should Be Reasonably Anticipated: The Sedona Conference suggests that the following factors be considered in determining whether litigation is or should be reasonably anticipated:

- The nature and specificity of the notice of potential claim or threat
- The person or entity making the claim
- The business relationship between the accused and accusing parties
- Whether the threat is direct, implied, or inferred
- Whether the party or counsel making the claim is known to be aggressive or litigious
- Whether a party who could assert a claim is aware of the claim
- The strength, scope, or value of a known, reasonably anticipated, or threatened claim
- Whether the organization has knowledge or information about similar claims
- The relevant experience in the industry with regard to such claims
- Reputable press or industry coverage of the issue, either directly pertaining to the organization or regarding complaints against others similarly situated
- Whether a party has retained counsel or is seeking advice of counsel in connection with defending against or filing a claim

- Whether an organization that is considering bringing a claim has begun to mark documents to indicate that they fall under the workproduct doctrine
- Whether a potential claimant has sent or received a demand, ceaseand-desist, or complaint letter⁴

§ 1.6 What Is Scope of Duty to Preserve?

§ 1.6:1 Federal Courts

Once the duty to preserve arises, a party must take reasonable steps to preserve what it knows or reasonably should know is relevant in the action and is reasonably likely to be requested during discovery. "[T]he duty persists throughout the litigation." *Davis SR Aviation, LLC v. Rolls-Royce Deutschland Ltd. & Co. KG*, No. A-10-CV-367 LY, 2012 WL 175966, at *2 (W.D. Tex. Jan. 20, 2012) (citing *Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001), among others).

§ 1.6:2 Texas State Courts

A party is not required to keep or retain every item or document in its possession, but it is required to preserve evidence that it knows or reasonably should know is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, or is the subject of a pending discovery sanction. *Adobe Land Corp. v. Griffin, L.L.C.*, 236 S.W.3d 351, 357–58 (Tex. App.—Fort Worth 2007, pet. denied). While parties are not required to take extraordinary measures to preserve evidence, the parties have a duty to exercise reasonable care in preserving potentially relevant evidence. *Adobe*, 236 S.W.3d at 359. "Evidence is relevant if (a) it has any tendency to make a fact more probable or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." Tex. R. Evid. 401. If there is some logical connection either directly or by inference between the evidence and a fact to be proved, the evidence is relevant. *See Service Lloyds Insurance Co. v. Martin*, 855 S.W.2d 816, 822 (Tex. App.—Dallas 1993, no writ).

As with the trigger date calculation, many court cases have wrestled with whether a party fully complied with its preservation obligations. Most courts look to what a

^{4.} The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & the Process*, 20 Sedona Conf. J. 381–82 (2019).

party knew or should have known about what claims or defenses would be raised and what information would be relevant. *See Marten Transportation, Ltd. v. Plattform Advertising, Inc.*, No. 14-cv-02464, 2016 WL 492743, at *10 (D. Kan. Feb. 8, 2016) (finding that duty to preserve did not extend to certain Internet search history because, at the time duty to preserve arose, there was no reason to believe plaintiff knew or should have known information would be relevant).

§ 1.7 Duty and Scope of Preservation and Federal Rules of Civil Procedure

As stated above, there is no specific rule that addresses when a duty to preserve attaches. That said, the Federal Rules of Civil Procedure require that parties discuss any issues relating to preserving discoverable information during the initial rule 26 conference. Fed. R. Civ. P. 26(f)(2). The purpose of discussing preservation is meant to reduce uncertainty and the risk of disputes that arise during discovery, particularly with regard to ESI. Fed. R. Civ. P. 26 advisory committee's note (¶ 22) to 2006 amendment. Considering the transient nature of ESI, parties are advised to discuss preservation obligations and the scope of data to be preserved as early as possible (even prior to the filing of the lawsuit).

The parties must include their proposals for preservation of ESI in the discovery plan. Fed. R. Civ. P. 26(f)(3)(C).

§ 1.8 How Does Concept of Proportionality Affect Preservation Obligations?

In amending Federal Rule of Civil Procedure 37, the advisory committee stated that a party could consider various factors in whether reasonable steps were taken to preserve data. Specifically, the note to the 2015 amendment states:

[Rule 37(e)] applies only if the information was lost because the party failed to take reasonable steps to preserve the information. Due to the everincreasing volume of electronically stored information and the multitude of devices that generate such information, perfection in preserving all relevant electronically stored information is often impossible. As under the current rule, the routine, good-faith operation of an electronic information system would be a relevant factor for the court to consider in evaluating whether a party failed to take reasonable steps to preserve lost information, although the prospect of litigation may call for reasonable steps to preserve
information by intervening in that routine operation. This rule recognizes that "reasonable steps" to preserve suffice; it does not call for perfection. The court should be sensitive to the party's sophistication with regard to litigation in evaluating preservation efforts; some litigants, particularly individual litigants, may be less familiar with preservation obligations than others who have considerable experience in litigation.

Another factor in evaluating the reasonableness of preservation efforts is proportionality. The court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts. A party may act reasonably by choosing a less costly form of information preservation if it is substantially as effective as more costly forms. It is important that counsel become familiar with their clients' information systems and digital data—including social media—to address these issues. A party urging that preservation requests are disproportionate may need to provide specifics about these matters in order to enable meaningful discussion of the appropriate preservation regime.⁵

Accordingly, it appears that when implementing its preservation obligations, a party may consider applying a proportionality analysis. Considerable caution and discretion, however, should be used in unilaterally taking actions that may later be construed as acts of spoliation. A party would be well advised to confer with opposing counsel and engage in a discussion of what preservation actions have been taken and what actions are not being considered because of proportionality concerns. Parties should be mindful that a miscalculation in applying the principles of proportionality "can lead to the permanent loss of relevant information." The Sedona Conference, *Commentary on Proportionality in Electronic Discovery* (2017).

The Sedona Conference offers the following advice:

Steps that can be taken by each party to meet its preservation obligations, where proportional, include:

i. in advance of litigation, having in place reasonable policies addressing legal preservation obligations that may arise;

^{5.} Fed. R. Civ. P. 37 advisory committee's notes to 2015 amendment (¶ 8-10).

- ii. identification of relevant custodians with knowledge of the matters in dispute;
- iii. discussion with custodians and other appropriate personnel to identify sources of unique ESI and other information relevant to the matter, including "non-custodial" sources;
- iv. preservation of the identified ESI;
- v. suspension of information retention policies that would otherwise result in the routine deletion of unique relevant ESI;
- vi. maintenance of relevant ESI in a reasonably accessible format; and
- vii. documentation of preservation efforts undertaken.⁶

§ 1.9 Preservation of Data and Reasonably Usable Form

Disputes often arise when a party unilaterally decides to preserve data in a format that may not be subject to an analysis of metadata or maintains the data in an otherwise unusable form. A party may be subject to sanctions or curative measures when it fails to take reasonable steps to preserve ESI. On the other hand, the 2015 advisory committee note to rule 37 makes clear that a "factor in evaluating the reasonableness of preservation efforts is proportionality." Fed. R. Civ. P. 37 advisory committee's note [¶ 10] to 2015 amendment. This analysis is fact intensive. Sometimes it can be found reasonable to preserve certain data in a certain format. However, when it appears that data is being preserved only partially or in a format that may obscure unique data, the argument fails. In the context of production, the advisory committee has stated:

"[T]he option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature."⁷

^{6.} The Sedona Conference, Commentary on Proportionality in Electric Discovery, 18 Sedona Conf. J. 152-53 (2017).

^{7.} Fed. R. Civ. P. 34 advisory committee's note [¶ 13] to 2006 amendment.

In Ashton v. Knight Transportation Inc., 772 F. Supp. 2d 772, 777 (N.D. Tex. 2011). the plaintiff claimed that Knight Transportation failed to preserve Qualcomm e-mailtype messages (among other investigatory items) between it and a driver surrounding the driver's automobile accident with Don Ashton on August 11, 2007, and what Knight did produce was illegible. Ashton, 772 F. Supp. 2d at 777. Knight had preserved messages in a screenshot-type fashion for August 13 and 14 following the accident but failed to do so August & through 12, which it claimed to be an "oversight." Ashton, 772 F. Supp. 2d at 789. As a result, the information could be retrieved only from a tape and exported into a spreadsheet format. Knight admitted that that format was easily manipulated, and information could have been deleted. Knight failed to explain why it had deleted the more readable Qualcomm records even though it had earlier received a written request to save them. Within a year, they were automatically deleted, proving that no effort was made to preserve the records from August 8 to 12 by screenshot, even in the face of a criminal investigation and a law enforcement agency request. The court held that by failing to preserve the Oualcomm data and then having deleted it for the hours surrounding the accident, the company violated its duty to preserve. Ashton, 772 F. Supp. 2d at 802.

§ 1.10 Preservation Orders

Courts generally disfavor the issuance of preservation orders and instead rely on the litigants' obligations to preserve relevant ESI and tangible items.⁸ However, where there is a danger of destruction absent a court order, courts are more prone to issue such an order. There is a split in the case law as to the proper standard for issuance of a protective order. Some courts have applied a temporary injunction standard—the movant must show irreparable injury and likelihood of success on the merits. Others have applied a two-prong test that requires the party seeking a preservation order to demonstrate that the data is necessary and that it is not unduly burdensome for the other party to preserve it.⁹

^{8. &}quot;The extremely broad discovery permitted by the Federal Rules depends on the parties' voluntary participation. The system functions because, in the vast majority of cases, we can rely on each side to preserve evidence and to disclose relevant information when asked (and sometimes even before then) without being forced to proceed at the point of a court order." *Klipsch Group, Inc. v. ePRO E-Commerce Ltd.*, 880 F.3d 620, 631 (2d Cir. 2018).

§ 1.11 Emerging Issues and Duty to Preserve— Ephemeral/Disappearing Messaging Apps

Parties have an obligation to preserve relevant, nonprivileged data. What happens when a party or its employees use ephemeral messaging applications, like Wickr, Telegram, and Snapchat? Typically, these apps use encrypted messages that instantly destroy themselves, but some of these apps allow the user to determine how long the messages exist before the app deletes them.

In *Waymo LLC v. Uber Technologies, Inc.*, No. C 17-00939 WHA, 2018 WL 646701 (N.D. Cal. Jan. 30, 2018), the court found that Uber sought to minimize its "paper trail" by using Wickr and decided to issue various jury instructions to address the failure to preserve the text messages and other discovery misconduct. The growing popularity of these types of apps, the acquiescence of companies to the use of these apps by their employees, and the difficulty in regulating their usage will present continuing challenges.

§ 1.12 Duty to Preserve When Documents Not in Party's Custody

Federal Rule of Civil Procedure 34 contemplates that a party may serve requests for production on a party, and a producing party must produce documents and ESI in its possession, custody, or control. Fed. R. Civ. P. 34(a). Does a nonparty owe any obligation to preserve documents or ESI?

In *Felman Production, Inc. v. Industrial Risk Insurers*, No. 3:09-0481, 2011 WL 4547012 (S.D. W. Va. Sept. 29, 2011), Felman operated a silicon manganese plant in which a furnace failed. Felman filed an insurance claim for business interruption due to the eight months it took to perform repairs. Industrial Risk Insurers (IRI) investigated for a full year and refused to settle the claim. Felman filed suit, and IRI counter-

§ 1.11

^{9.} See Toussie v. Allstate Insurance Co., No. 15 CV 5235 (ARR) (CLP), 2018 WL 2766140, at *7 (E.D.N.Y. June 8, 2018) ("The Court has carefully considered the cases cited by the parties and agrees with other courts that have rejected the preliminary injunction standard in the context of orders to preserve relevant evidence for use in discovery and at trial. Unlike a preliminary injunction, a preservation order has little to do with the substantive merits of any claim or defense; instead, such an order enforces the parties' pre-existing, independent obligations to preserve relevant evidence for use in discovery and at trial, thereby ensuring the integrity and fairness of the adjudicative process. Consistent with that purpose, the Court agrees that a version of the balancing test is the appropriate standard by which to determine whether to continue the preservation order. Thus, the Court will consider: 1) the danger of destruction absent a court order, 2) whether any irreparable harm is likely to result to the party seeking preservation in the absence of an order, and 3) the burden of preserving the evidence."). See also OOO Brunswick Rail Management v. Sultanov, No. 5:17-CV-00017-EJD, 2017 WL 67119, at *1 (N.D. Cal. Jan. 6, 2017) (same factors applied).

Duty to Preserve

claimed for fraud, basing its allegations on documents discovered between Felman and an entity called Privat wherein the two companies discussed backdating contract orders and other efforts to bolster Felman's insurance claim. Felman actively concealed its relationship with Privat but inadvertently produced other documents that referred to the fact that Privat, a Ukrainian organization, was Felman's controlling entity during the relevant time frame. Felman alleged, however, that it had no legal duty to preserve Privat's documents because, at the time suit was filed, the consulting relationship between Privat and Felman had ended and that it had no control over Privat's documents. *Felman*, 2011 WL 4547012, at *11.

The court held that it was not unreasonable for Felman to institute a litigation hold to key Privat players. *Felman*, 2011 WL 4547012, at *12. It had already been determined that Felman's outside counsel was in contact with these key players and could have issued a litigation hold without significant effort. Privat's location in the Ukraine represented a minimal barrier to preserving documents. "Your clients need to understand that they chose this country to do business, and they chose this court to file a lawsuit, and they will be held to the standards of this [country] and these rules, not their culture and their rules." *Felman*, 2011 WL 4547012, at *12. Accordingly, the court held that Felman had a duty to preserve Privat's documents.

§ 1.13 Conclusion

Parties cannot ignore ESI when the duty to preserve arises. They must educate themselves about what relevant ESI may exist and how it can be preserved; then they must preserve that ESI and remain vigilant that such ESI is subject to an effective legal hold. Only then will their actions be deemed reasonable in the face of spoliation accusations.



Chapter 2

Litigation Holds

Lawrence Morales II

§ 2.1 Definition

A litigation hold is a written directive advising custodians of certain documents and electronically-stored information ("ESI") to preserve potentially relevant evidence in anticipation of future litigation. Also called "preservation letters" or "stop destruction requests," these communications basically advise of the possibility of future litigation and identify relevant documents and ESI which should be preserved.¹

§ 2.2 Issuance of a Litigation Hold Assists in the Preservation of Evidence and Helps Stave Off Allegations of Spoliation of Evidence

Rule 37(e) authorizes courts to impose sanctions under certain circumstances if "a party fail[s] to take reasonable steps to preserve" electronically stored information.² To avoid sanctions or the imposition of curative measures, counsel and clients must take deliberate steps to ensure that relevant records and ESI are preserved, collected, and produced. One of these steps is distribution of a litigation hold memorandum that instructs custodians to (1) preserve all relevant documents and ESI and (2) suspend document retention/destruction policies that may delete such data. However, the litigation hold memorandum is just one step—albeit an important step—in satisfying the duty to preserve. Contrary to common belief, the litigation hold memorandum is not, by itself, sufficient to satisfy a party's preservation duties. "A party's discovery obligations do not end with the implementation of a 'litigation hold'—to the contrary, that's only the beginning."³ Counsel must also oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce relevant documents.⁴

4. Zubulake, 229 F.R.D. at 432.

^{1.} Stephen F. Stacy, *Litigation Holds: Ten Tips in Ten Minutes*, www.ned.uscourts.gov/ internetDocs/cle/2010-07/LitigationHoldTopTen.pdf (last visited May 27, 2019).

^{2.} Fed. R. Civ. P. 37(e).

^{3.} Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) (Zubulake V).

If done properly, the steps required to satisfy the duty to preserve are time-consuming, expensive, and potentially disruptive to clients' operations. Moreover, because many attorneys do not take these steps, clients may be uncooperative and may perceive counsel's preservation efforts as a method to increase fees. However, the potential consequences for failing to satisfy the duty to preserve cannot be understated. Indeed, litigants could face serious sanctions or costly curative measures for failing to properly preserve relevant documents.⁵ Therefore, it is imperative that counsel advise their clients in their litigation hold memorandum of the stakes involved in preserving all relevant records and obtain their clients' full cooperation in satisfying their preservation duties.

An example of numerous failures to preserve documents is found in *E.I. du Pont de Nemours & Co. v. Kolon Industries, Inc.*, a case involving theft of trade secrets. The court held that the defendant, a Korean company:

breached its duty to preserve when key employees, who were directly implicated in [the company]'s efforts to recruit consultants . . . and obtain information about Kevlar for use in developing Heracron, deleted files and email items from their personal computers in the days after DuPont filed the action and after being apprised of their duty to preserve relevant information.⁶

The court was quick to note that while two separate litigation holds were issued, both were insufficient.⁷ The first litigation hold was issued only to upper-level employees, with no instruction to filter this hold down to subordinates.⁸ Although the litigation hold advised that recipients might want to share the hold with other personnel, there was no evidence showing that the contents or the subject matter of the litigation hold was communicated to other employees.⁹ The second hold was issued in English to

- 6. Kolon Industries, 803 F. Supp. 2d 469, 500 (E.D. Va. 2011).
- 7. 803 F. Supp. 2d at 479.
- 8. 803 F. Supp. 2d at 479.

^{5.} See Keithley v. Home Store.com, Inc., No. C-03-04447 SI (EDL), 2008 WL 3833384 (N.D. Cal. Aug. 12, 2008); United States v. Trinity Industries, Inc., No. 2:12-CV-89, 2014 WL 12603247 (E.D. Tex. July 11, 2014) (faulting party for failure to institute and enforce a litigation hold or take reasonable steps to ensure relevant documents were preserved); see also Merck Eprova AG v. Gnosis S.P.A., No. 07 Civ. 5898 (RJS), 2010 WL 1631519 (S.D.N.Y. Apr. 20, 2010) (awarding plaintiff attorneys' fees, costs, and a \$25,000 fine because the defendant did not issue a litigation hold or prevent the automatic deletion of relevant e-mails); Mercedes-Benz USA, LLC v. Carduco, Inc., 562 S.W.3d 451 (Tex. App.—Corpus Christi–Edinburg 2016), rev'd on other grounds, 583 S.W.3d 553 (Tex. 2019) (failure to issue a litigation hold even after being served requests for production and merely allowing employees to submit responsive documents considered in affirming large punitive damages awarded).

Litigation Holds

Korean employees without consideration for the language barrier that undoubtedly existed.

To make matters worse, the court found that "key employees intentionally, and in bad faith, deleted files and email items from their personal computers after they learned of DuPont's Complaint."¹⁰ Specifically, several employees of the defendant company "marked items in their personal e-mail accounts for deletion by taking screenshots, circling relevant materials, and notating the documents with directions such as 'Delete,' 'Need to Delete,' and 'Get Rid of."¹¹

As a sanction, the court in the *DuPont* matter awarded \$4.5 million in attorney's fees to DuPont, one of the largest attorney fee judgments in a spoliation case to date.

§ 2.3 Crafting an Effective Litigation Hold

This section identifies the standards for crafting an effective litigation hold memorandum and discusses cases where a party's litigation hold was held to be insufficient. In addition, this section compiles litigation hold practices that, if implemented, would have allowed these parties to escape sanctions. These practices include—

- 1. meeting with key players and counsel to determine the issues that may be raised in the litigation;
- 2. identifying the custodians who are likely to have records relevant to these issues;
- 3. conferring with information technology personnel to identify where these records are stored;
- 4. distributing an adequate litigation hold memorandum to all employees and third parties under the client's control who may possess relevant records;
- 5. suspending procedures that may automatically delete relevant records;
- 6. monitoring and tracking clients and third parties to ensure they are complying with the litigation hold;¹² and

- 10. 803 F. Supp. 2d at 501.
- 11. 803 F. Supp. 2d at 501.

12. See Major Tours, Inc. v. Colorel, No. 05-3091 (JBS/JS), 2009 WL 2413631, at *2 (D.N.J. Aug. 4, 2009) ("Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce relevant documents.").

^{9. 803} F. Supp. 2d at 479.

7. revising and redistributing the litigation hold memorandum as issues in the litigation develop and expand.

Some may characterize these measures as best practices; however, the courts that have imposed sanctions for failing to implement sufficient litigation holds have admonished the parties for failing to take one or more of these preservation measures. So, litigants that neglect these steps proceed at their own peril.

§ 2.4 Implementing an Effective Litigation Hold

§ 2.4:1 Must Litigation Hold Letters Be in Writing?

The concept of "litigation holds" as a method for litigants to satisfy their preservation obligations was popularized by Judge Shira A. Scheindlin's 2003 decision in *Zubulake v. UBS Warburg LLC (Zubulake IV)*, in which the court noted that "[o]nce a party reasonably anticipates litigation, it must suspend its routine document retention/ destruction policy and put in place a 'litigation hold."¹³ In a subsequent 2010 decision in *Pension Committee v. Banc of America Securities, LLC*, the same court held that "the failure to issue a written litigation hold constitutes gross negligence because the failure is likely to result in the destruction of relevant information."¹⁴

However, not all courts require a written litigation hold.¹⁵ For example, in *Davis SR Aviation, LLC v. Rolls-Royce Deutschland, Ltd. & Co. KG*, a Texas district court stated: "the failure to send a written 'litigation hold' memo is largely irrelevant in the actual spoliation analysis because—litigation hold or not—to show spoliation one must still demonstrate the loss or destruction of evidence."¹⁶ In addition, one court opined that written litigation hold letters may be counterproductive in small organizations because "such a hold would likely be more general and less tailored to individual records custodians than oral directives could be."¹⁷ And even Judge Scheindlin has clarified that if you are a company of one, you "don't [need to] write a letter to yourself."¹⁸ Further, the 2015 amendment advisory committee notes to Rule 37(e) state

15. The Sedona Conference, *The Sedona Conference Commentary on Legal Holds: The Trigger & The Process*, 11 Sedona Conf. J. 265 (2010).

^{13. 220} F.R.D. 212, 218 (S.D.N.Y. 2003).

^{14. 685} F. Supp. 2d 456, 460 (S.D.N.Y. 2010); see also GenOn Mid-Atlantic, LLC v. Stone & Webster, Inc., 282 F.R.D. 346 (S.D.N.Y. 2012) (finding "a degree of culpability sufficient to permit the imposition of sanctions" where company failed to issue written litigation hold after it contemplated litigation). But see Chin v. Port Authority of New York & New Jersey, 685 F.3d 135 (2d Cir. 2012) (in which the court held that the failure to issue a written litigation hold does not constitute gross negligence per se, but is rather one factor to consider in determining whether to issue sanctions).

Litigation Holds

that the "court should be sensitive to the party's sophistication with regard to litigation in evaluating preservation efforts; some litigants, particularly individual litigants, may be less familiar with preservation obligations than others who have considerable experience in litigation."¹⁹ However, small organizations are by no means immune from sanctions for failing to preserve evidence. Indeed, at least one court has sanctioned a small company \$10,000 for, among other things, failing to issue a written litigation hold.²⁰

In summary, while there may be a disagreement between courts over whether *written* litigation holds are required, the safest practice is to disseminate one. If there is no written litigation hold memorandum, counsel will likely be unable to precisely identify the dates and the recipients of any oral directives to preserve evidence. As the saying goes, "if it's not written, it didn't happen." To avoid this presumption, counsel should always distribute a litigation hold memorandum and, as discussed below, take steps to verify that it was received and followed.

§ 2.4:2 What Should Be Included in the Litigation Hold Memorandum?

The purpose of a litigation hold memorandum is to (1) identify the litigation, (2) specify the parties to the litigation, (3) specifically identify the documents to be preserved, (4) suspend automatic document retention/destruction policies that may delete relevant information, (5) provide a contact point within the company to answer questions, (6) explain the importance of compliance with the hold memorandum, and (7) provide a formal process to verify the recipient received the memorandum and is taking steps to comply with it.²¹ While several of these items are self-explanatory (nos. 1, 2, 5, and

^{16.} No. A-10-CV-367 LY, 2012 WL 175566, at *3 n.3 (W.D. Tex. Jan. 12, 2012); see also Flanders v. Dzugan, No. CIV.A 12-1481, 2015 WL 5022734, at *5–6 (W.D. Pa. Aug. 24, 2015) (stating failure to institute a litigation hold without a showing of bad faith not sufficient despite foreseeability of litigation); Kinnally v. Rogers Corp., No. CV-06-2704-PEX-JAT, 2008 WL 4850116, at *7 (D. Ariz. Nov. 7, 2008) (holding that sanctions do not lie merely because of the "absence of a written litigation hold" when a party has taken "the appropriate actions to preserve evidence."); Orbit One Communications, Inc. v. Numerex Corp., 271 F.R.D. 429, 441 (S.D.N.Y 2010) ("Indeed, under some circumstances, a formal litigation hold may not be necessary at all.").

^{17.} Orbit One, 271 F.R.D. at 441.

^{18.} Judge Shira A. Scheindlin, address at Georgetown University Law Center Advanced E-Discovery Institute (Nov. 18–19, 2010).

^{19.} Fed. R. Civ. P. 37, 2015 advisory committee's notes.

^{20.} See Passlogix, Inc. v. 2FA Technology, LLC, 708 F. Supp. 2d 378, 422 (S.D.N.Y. 2010).

^{21.} See Shira A. Scheindlin et al., *Electronic Discovery and Digital Evidence, Cases and Materials* 2d ed., at 191 (West Academic Publishing, 2012).

6), the remaining items are discussed below because they have been cited as reasons for a party's failure to comply with their preservation duties.

Specifically Identifying the Documents to Be Preserved: Notably, "[t]he preservation obligation runs first to counsel, who has a duty to advise his client of the type of information potentially relevant to the lawsuit and of the necessity of preventing its destruction."²² To satisfy its preservation obligations, an organization "must inform its officers and employees of the actual and anticipated litigation, and identify for them the kinds of documents that are thought to be relevant to it."²³ "It is no defense to suggest . . . that particular employees were not on notice To hold otherwise would permit an agency, corporate officer, or legal department to shield itself from discovery obligations by keeping its employees ignorant."²⁴

A standard cookie-cutter litigation hold memorandum will not suffice. Rather, to satisfy their preservation obligations, counsel must tailor the contents of each litigation hold memorandum to describe the specific issues and documents that are relevant to each case. In fact, a common shortcoming cited by courts concerning litigation holds is the failure to adequately instruct employees what types of documents are relevant. For example, in *Jones v. Bremen High School District 228*, the court sanctioned the defendant because it only instructed three individuals to cull through their personal documents and preserve anything related to the case.²⁵ However, these individuals were not provided any specific guidance on how to conduct their searches or how to determine what documents were relevant. Although there was no evidence of bad faith, the court sanctioned the defendant with an adverse jury instruction and with an order to pay plaintiff's costs and attorney's fees because there was a "distinct possibility that emails relevant to plaintiff's case were destroyed."²⁶

Similarly, in *Pension Committee*, Judge Scheindlin held that a general instruction to collect and preserve evidence did not meet the standard for a litigation hold because it did not direct employees to preserve all relevant paper documents, and did not "create a mechanism for collecting the preserved records so that they [could] be searched by someone other than the employee."²⁷ Counsel's instruction only directed the employ-

- 24. Triple 8 Palace, 2005 WL 192557, at *6.
- 25. No. 08 C 3548, 2010 WL 2106640, at *8 (N.D. Ill. May 25, 2010).
- 26. Bremen High School, 2010 WL 2106640, at *8.

^{22.} Heng Chan v. Triple 8 Palace, No. 03CIV6048 (GEL) (JCF), 2005 WL 192557, at *6 (S.D.N.Y. Aug. 11, 2005).

^{23.} Cannata v. Wyndham Worldwide Corp., No. 2:10-cv-00068-PMP-LRL, 2011 WL 3495987, at *2 (D. Nev. Aug. 10, 2011) (citation omitted).

Litigation Holds

ees to search and select records that employees thought were responsive to discovery requests; however, the instruction failed to instruct the plaintiffs not to destroy documents. Consequently, Judge Scheindlin held that plaintiffs were grossly negligent, and imposed sanctions.²⁸

It is generally not a best practice to allow individual employees to determine which documents are relevant. This practice is fraught with potential problems, such as under-preservation, over-preservation, and intentional or negligent deletion of data. Nevertheless, some courts have rejected the argument that it was per se inadequate to allow individual employees the ability to determine which documents were relevant, considering that the employees in question were given detailed instructions as to what type of documents to retain.²⁹

To adequately identify the types of relevant documents that may exist in a particular case, it is advisable for counsel to convene a "claims and defense assessment" meeting to isolate the issues that may be raised in the potential litigation.³⁰ The purpose of the assessment meeting is to compile a list of the types of documents that may be relevant to the claims and defenses in the litigation and to pinpoint the individuals who may have those documents. The resulting list of documents should then be inserted in the litigation hold memorandum.

The claims and defense assessment meeting will typically include in-house counsel (if any), outside counsel, and the key players involved in the dispute.³¹ Counsel's role during the assessment meeting is to educate the client on the claims and defenses asserted, and to describe the specific elements required for each claim and defense. Thus, it is important that counsel familiarize themselves with the law relating to the relevant claims and defenses before the assessment meeting. Because a productive assessment meeting takes preparation, it may not be possible to have the meeting immediately after the preservation-triggering event. Therefore, it is wise to first issue a high-level general hold notice to all employees notifying them of the need to preserve, pending more specific instruction to follow shortly.³²

31. See Scheindlin, Electronic Discovery, at 188.

^{27.} Pension Committee, 685 F. Supp. 2d at 473.

^{28.} Pension Committee, 685 F. Supp. 2d at 473.

^{29.} See New Mexico Oncology & Hematology Consultants, Ltd. v. Presbyterian Healthcare Services, No. 1:12-CV-00526 MV/GBW, 2017 WL 3535293, at *3 (D.N.M. Aug. 16, 2017); see also Mirmina v. Genpact LLC, No. 3:16CV00614(AWT), 2017 WL 3189027, at *2 (D. Conn. July 27, 2017) (counsel coordinated and supervised individual custodian's search for ESI).

^{30.} See Scheindlin, Electronic Discovery, at 188.

Suspending Document Retention and Destruction Policies: Once litigation is anticipated, parties must at the very least suspend their routine document retention and destruction policies and establish measures to ensure the preservation of relevant documents and information.³³ This point was made clear in Judge Scheindlin's decision in *Pension Committee*, in which the defendants moved for sanctions "alleging that each plaintiff failed to preserve and produce documents—including those stored electronically—and submitted false and misleading declarations regarding their document collection and preservation efforts."³⁴ The court held that plaintiffs' continued deletion of electronically stored information after the duty to preserve was triggered amounted to gross negligence and the court therefore imposed appropriate sanctions.³⁵

Providing a Formal Tracking and Verification Process: "While instituting a 'litigation hold' may be an important first step in the discovery process, the obligation to conduct a reasonable search for responsive documents continues through the litigation."³⁶ A litigation hold, without more, will not suffice to satisfy the "reasonable inquiry" requirement in Rule 26(b)(2) of the Federal Rules of Civil Procedure.³⁷ "Counsel retains an ongoing responsibility to take appropriate measures to ensure that the client has provided all available information and documents which are responsive to discovery requests."³⁸

How does counsel ensure that the client has received and followed the litigation hold memorandum? First, numerous software programs are commercially available that allow litigants to, among other things, track litigation hold letters. Other companies spare the expense of purchasing software and track litigation holds manually through spreadsheets or other informal methods. Another effective method is to require each custodian to sign a certification/acknowledgment that the litigation hold memorandum has been received, understood, and implemented, similar to the following:

- 35. Pension Committee, 685 F. Supp. 2d at 463.
- 36. Cache La Poudre Feeds, 244 F.R.D. at 630.
- 37. Cache La Poudre Feeds, 244 F.R.D. at 630.
- 38. Cache La Poudre Feeds, 244 F.R.D. at 630.

^{32.} See Scheindlin, Electronic Discovery, at 188.

^{33.} Pension Committee, 685 F. Supp. 2d at 466; see also Peskoff v. Faber, 244 F.R.D. 54, 60 (D.D.C. 2007); Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 629 (D. Colo. 2007) (noting that once litigation hold has been established, party cannot continue routine procedures that effectively ensure potentially relevant and readily available electronically stored information is destroyed).

^{34.} Pension Committee, 685 F. Supp. 2d at 463.

Acknowledgment³⁹

(Please provide to your general counsel or your immediate supervisor)

I acknowledge I have read the above attached Litigation Hold memorandum. I will forthwith conduct a reasonable search for responsive documents and electronic data. I will preserve any such electronic data and paper documents. I will not delete any data from any locations that I believe may contain responsive electronic data. I understand that this preservation request is on-going and requests the continuing preservation of data, including data created or received both before and after receipt of the Notice.

Employee signature

Employee name

Date

In addition to requiring that custodians sign certifications that they have read, understood, and will comply with the litigation hold memorandum, it is wise to schedule interviews with each custodian to review what data the custodian holds and how it must be preserved.⁴⁰ Moreover, taking these measures creates a well-documented trail of counsel's efforts to preserve all relevant documents, which will provide compelling evidence in any potential spoliation battle.

§ 2.5 Are Litigation Hold Memoranda Discoverable?

"In general, unless spoliation is at issue, a litigation hold letter is not discoverable, particularly where it is shown that the letter includes material protected by the attorney-client privilege or the work product doctrine."⁴¹ However, the basic details surrounding the litigation hold are typically not privileged.⁴² A party is entitled to know what kinds and categories of electronically stored information the opposing party was instructed to preserve and collect, and what specific actions they were instructed to take.⁴³ Most courts have concluded that litigation hold letters or memos are protected by the attorney-client privilege if prepared by counsel and directed to the client. How-

25

^{39.} Scheindlin, Electronic Discovery, at 138.

^{40.} Scheindlin, Electronic Discovery, at 193.

ever, opposing counsel are generally entitled to inquire in depositions "into the facts as to what the employees receiving the [document retention notices] have done in response; i.e., what efforts they have undertaken to collect and preserve applicable information."⁴⁴

For example, in *Cannata v. Wyndam Worldwide Corp.*,⁴⁵ the plaintiffs alleged that they were subjected to widespread sexual harassment and discrimination. The plaintiffs served the defendants with a Rule 30(b)(6) deposition notice, wherein they requested to depose a corporate representative concerning the company's litigation hold and electronically stored information.⁴⁶ The defendant filed a motion for protective order, requesting that the court limit the scope of the litigation hold topic to the identity of persons who received litigation hold notices and the information regarding what such recipients were instructed to do to preserve evidence.⁴⁷

The court denied the defendant's motion for protective order, stating that "[a]lthough the [litigation hold] letters themselves may be privileged, the basic details surrounding the litigation hold are not."⁴⁸ "To the extent . . . that defendants seek 'to foreclose any inquiry into the contents of those [litigation hold] notices at deposition or through other means, such a position is not tenable."⁴⁹ The court determined that plaintiffs'

47. 2011 WL 3495987, at *2.

^{41.} Cannata v. Wyndham Worldwide Corp., No. 2:10-cv-00068-PMP-LRL, 2011 WL 3495987, at *2 (D. Nev. Aug. 10, 2011); see also Ingersoll v. Farmland Foods, Inc., No. 10-6046-CV-SJ-FJG, 2011 WL 1131129, at *17 (W.D. Mo. Mar. 28, 2011); In re Ebay Seller Antitrust Litigation, No. C 07-01882 JH (RS), 2007 WL 2852364, at *2 (N.D. Cal. Oct. 2, 2007); Gibson v. Ford Motor Co., 510 F. Supp. 2d 1116, 1123 (N.D. Ga. 2007) (finding that defendants are not required to produce litigation hold letters because "[n]ot only is the document likely to constitute attorney work-product, but its compelled production could dissuade other businesses from issuing such instructions in the event of litigation"); Muro v. Target Corp., 250 F.R.D. 350, 360 (N.D. Ill. 2007) (denying plaintiff's objection to magistrate's ruling that Target's litigation hold notices are subject to the attorney-client privilege and to work-product protection); Turner v. Resort Condominium International, LLC, No. 1:03-cv-2025-DFH-WTL, 2006 WL 1990379, at *7–8 (S.D. Ind. July 13, 2006) (accepting defendant's assertion that its litigation hold document is privileged and denying plaintiff's motion to compel defendant to produce the document in discovery).

^{42.} Cannata, 2011 WL 3495987, at *3.

^{43.} *Cannata*, 2011 WL 3495987, at *3; *see also* Fed. R. Civ. P. 26(b)(2), advisory committee's note ("The responding party must also identify, by category or type, the sources potentially responsive information that it is neither searching nor producing.").

^{44.} Shenwick v. Twitter, Inc., No. 16-CV-05314-JST (SK), 2018 WL 833085, at *4 (N.D. Cal. Feb. 7, 2018).

^{45. 2011} WL 3495987, at *1.

^{46. 2011} WL 3495987, at *1.

^{48. 2011} WL 3495987, at *3.

^{49. 2011} WL 3495987, at *2 (citation omitted).

Litigation Holds

requests were reasonable and would "allow the parties to craft a narrow, manageable ESI plan."⁵⁰ The court also noted that defendants' litigation hold letter and practices may actually benefit the defendants if questions ever arise concerning their efforts to preserve ESI.⁵¹

Although litigation hold letters are generally privileged, the prevailing view is that when spoliation occurs, the letters are discoverable.⁵² For example, in *Major Tours, Inc. v. Colorel*, the plaintiffs requested that the defendants produce their litigation hold letters to allow an examination of the scope of the defendants' document production and whether they spoliated relevant evidence.⁵³ The plaintiffs claimed that the litigation hold letters were no longer subject to the attorney-client privilege or the work-product exemption because they had made a preliminary showing of spoliation.⁵⁴ The defendants disagreed and filed a motion for protective order.⁵⁵

The court denied the defendants' motion for protective order, concluding that there had been a "preliminary showing of spoliation of evidence."⁵⁶ The court largely based its finding on the testimony of the defendants' corporate representative.⁵⁷ Specifically, when asked whether he was advised by his attorneys to preserve his relevant e-mails, the corporate representative testified that he was "probably" told by his lawyers to do so, but admitted, "I don't sa[v]e anything."⁵⁸ Another defense witness testified that, "no one ever talked to her about creating a litigation hold policy and that she was not sure what a litigation hold policy was."⁵⁹ Based on this testimony, the court held there

52. See Major Tours, 2009 WL 2413631, at *2; United Medical Supply Co., Inc. v. United States, 77 Fed. Cl. 257 (Fed. Cl. 2007) (ordering defendants to file and produce copies of their litigation hold notices after plaintiffs made preliminary showing of spoliation); Keir v. Unumprovident Corp., No. 02-CV-8781 (DLC), 2003 WL 21997747, at *6 (S.D.N.Y. Aug. 22, 2003) (allowed detailed analysis of emails pertaining to defendant's preservation efforts after finding that electronic records that had been ordered preserved had been erased); Zubulake V, 229 F.R.D. at 425 nn.15–16 (disclosing details of counsel's litigation hold communication after discovery that at least one e-mail had never been produced); Cache La Poudre, 244 F.R.D. at 634 (permitting plaintiff to take rule 30(b)(6) deposition to explore procedures defendants' counsel took "to identify, preserve and produce responsive documents" after finding that defendants expunged hard drives of several former employees after present litigation had begun).

- 53. 2009 WL 2413631, at *1.
- 54. 2009 WL 2413631, at *1.
- 55. 2009 WL 2413631, at *1.
- 56. 2009 WL 2413631, at *3.
- 57. 2009 WL 2413631, at *3.
- 58. 2009 WL 2413631, at *3.
- 59. 2009 WL 2413631, at *3.

^{50. 2011} WL 3495987, at *3.

^{51. 2011} WL 3495987, at *3.

had been a preliminary showing of spoliation and ordered defendants to produce their litigation hold letters.⁶⁰

§ 2.6 Lifting Litigation Holds

A litigation hold may be released or lifted after the litigation is finally resolved, assuming that the preserved data is not required to be preserved pursuant to some federal or state regulation or relevant to any other existing or anticipated litigation.⁶¹ However, the decision to lift a litigation hold should be made only after conducting due diligence to ensure that the preserved data is not relevant to any claims or defense for other litigation matters, including audits and investigations.⁶²

§ 2.7 Sample Litigation Hold Notice

DOCUMENT PRESERVATION NOTICE63

IMMEDIATE ACTION REQUIRED

To: Distribution List

From: General Counsel

The Company has recently been sued by Jane Doe for age discrimination and alleged violations of the Fair Labor Standards Act ("FLSA"). Specifically, Ms. Doe alleges that she was not promoted to a sales manager in June 2013 because of her age, and that she was required to work off-theclock and, consequently, was not paid wages and/or overtime for all hours worked. We intend to vigorously defend this lawsuit.

The law requires us to take immediate steps to preserve all paper records and electronic data that is relevant to the litigation. Paper records and electronic data (including duplicates) must be preserved at all storage locations including your office computer, home computers, and other portable electronic media such as discs and thumb drives. Failure to preserve all paper records and electronic data may result in legal sanctions, including, but not limited to, fines, instructions to the jury that any deleted data would have

63. Scheindlin, Electronic Discovery, at 189-90.

^{60. 2009} WL 2413631, at *5.

^{61.} Scheindlin, Electronic Discovery, at 194; see also chapter 1 of this book.

^{62.} Scheindlin, Electronic Discovery, at 194.

§ 2.7

been harmful to our defense, and even a finding that the Company is precluded from defending Ms. Doe's case.

Please immediately review the following list of categories of documents (paper and electronic data) which must be preserved. All electronic data and paper documents including drafts, e-mail negotiations and communications related to or about any of these categories must be preserved.

- 1. All documents contained in Ms. Doe's personnel file.
- 2. All documents related to any contract, negotiation, or communication with Ms. Doe.
- 3. All job descriptions for the positions held by Ms. Doe during her employment with the company.
- 4. All job descriptions for the positions that Ms. Doe applied for during her employment with the company.
- 5. All communications with Ms. Doe concerning the hours she worked.
- 6. All timesheets and other records reflecting the hours worked by Ms. Doe.
- 7. All applications submitted for the sales manager position sought by Ms. Doe.
- 8. All performance evaluations evaluating the work performance of Ms. Doe.
- 9. All performance evaluations evaluating the work performance of all applicants for the sales manager position sought by Ms. Doe.
- 10. All notes, memoranda, and spreadsheets related to Ms. Doe.
- 11. All communications concerning the selection of a candidate to fill the sales manager position sought by Ms. Doe.
- 12. All work schedules for Ms. Doe during her employment with the Company.

Please determine immediately whether you have in your possession, custody, or control any paper or electronic data about, concerning, or related to any of the above preservation categories. Such paper documents or electronic data are called responsive documents or data.

Please determine whether any responsive data is located on your laptop or office computer, home computer, iPhone, iPad, PDA, discs, CDs, DVDs,

memory sticks or thumb drives, voicemail, or any other electronic storage location. Please immediately suspend the deletion (manual or automatic) of relevant electronic data from any location where you believe responsive data may be found.

With respect to paper documents, please check all your office files and home files. Please immediately suspend the destruction of any responsive paper documents.

This litigation hold should remain in place until you are notified otherwise by written correspondence from my office.

If you have any doubts about what paper or electronic data to preserve, please contact me. If you have any responsive paper documents, please immediately advise your supervisor. If you have any responsive electronic data held or stored at any location or on any media other than your office laptop, please immediately advise your supervisor.

I acknowledge receipt of this document prescription notice, agree to comply with this request, and understand this request.

Employee name

Please keep a copy of this notice and return the signed original to

Chapter 3

Computer Usage Policies, Records Management, and Information Governance

Jonathan Lass

§ 3.1 Introduction

Topics covered in this chapter include information governance management issues in the context of electronic discovery ("e-discovery"), including how document retention policies, records management, and computer usage policies affect a party's risk management position when facing e-discovery. This chapter will conclude with recommendations helpful to you or your clients concerning specific computer usage policies that will assist you in developing an effective information governance and document management and retention policy to best protect you or your clients from e-discovery issues that may arise during litigation, investigations, or audits.¹

Parties involved in litigation are concerned with e-discovery as a means to obtain information about the adverse party's claims or defenses. To avoid sanctions for failing to preserve data relevant to the litigation or a presumption that deleted data was beneficial to the claims of the adverse party, companies and agencies have developed document retention policies ("DRPs") aimed at regulating the destruction of data, including the most prevalent type of data, electronically stored information ("ESI"), that the company or agency holds in its or its employees' possession. Companies or agencies have adopted DRPs that, if effective, reflexively respond to receipt of litigation hold letters from adverse parties in litigation, thereby avoiding failure-to-preserve-data claims (also known as spoliation claims) from requesting parties.

§ 3.2 Computer Usage Policies

While the ability to save large amounts of data at lower costs per terabyte is appealing to commercial and public entities, it also means that these companies and agencies are

^{1.} Additional helpful guidance may be found in The Sedona Conference, *Commentary on Information Governance, Second Edition*, 20 Sedona Conf. J. 95 (April 2019), https://thesedonaconference.org/publication/Commentary_on_Information_Governance, and the Information Governance Reference Model (IGRM). Information Governance Reference Model, EDRM, www.edrm.net/ frameworks-and-standards/information-governance-reference-model/.

storing increasingly larger amounts of data, much of which is no longer useful to the organization. The risk of holding so much unnecessary data becomes apparent when a company or agency is the subject of litigation, an investigation, or an audit wherein large amounts of ESI will need to be preserved, collected, and later reviewed to determine whether it is within the scope of the subject litigation, investigation, or audit, and then whether the ESI is subject to a privilege, such as the attorney-client privilege or the attorney work product privilege. Information governance policies assist companies in regulating the placement and volume of stored data, in most cases ESI. Computer usage policies, namely DRPs, address the problem of managing the accumulation of ESI and the systematic processes that purge unnecessary data on a regular basis.

An effective computer usage policy provides clear rules for storage of data (that is, proper places for storage and types of data to be stored), timing of deletion of such data, and suspension of deletion of data in the context of a legal hold that pertains to an actual or threatened litigation, audit, or investigation.

To be effective, computer usage policies must clearly explain the rules for storage of electronically stored data and have systems that congruently act to initially deploy and then manage the computer usage policies. In the face of litigation hold letters or requests for production, having computer usage policies pays for itself several times over.

Companies should take seriously best practices and the steps to mitigate exposure when preservation and production of ESI is required. Employees should review and acknowledge company computer usage policies upon the date of employment. Such policies generally cover the following areas, which are calculated to provide the best return on investment to reduce legal risk.

§ 3.2:1 No Right of Privacy

For company employees residing in the United States, it is standard for companies to place a disclaimer that any electronic communications and any documents stored on the company's servers or computers shall be the property of the company and subject to review and use by the company, and that the employee should not expect any right of privacy with respect to electronic communications.

§ 3.2:2 Use of Internet on Company Devices

Internet usage policies typically request that employees refrain from inappropriate use of the Internet, including accessing websites that have inappropriate, harassing, sexually explicit, or illegal content. Compliance reduces a company's legal risk.

§ 3.2:3 Storage of Personal Documents on Company Devices

Companies' computer usage policies typically include a restriction that company devices issued to employees should not be used for nonbusiness purposes. Further, more sophisticated company policies include a provision specifically restricting employees from storing personal documents or e-mails.

§ 3.2:4 Storage of Work Documents on Personal Devices

The concept explored here relates to bring-your-own-device ("BYOD") policies and practices that encourage employees tc not only bring their personal devices to work, but also use these personal devices to engage in work activities and communications on behalf of the company. BYOD policies are fraught with e-discovery issues, especially within the context of preservation of documents and spoliation, which could result in incomplete responses to requests for production in some cases, and discovery of ESI that should have been deleted pursuant to the company's DRP. BYOD policies should address the employee's ability to transfer ESI to a personal e-mail account or device, and, presuming transfer of ESI onto a personal device is allowed, then procedures should be implemented to comply with the DRP including transferring ESI stored on the personal device to the employer upon the employee's termination of employment.

§ 3.2:5 Use of E-Mails

E-mail usage policies typically focus on prohibiting (or limiting) personal use of email. E-mail usage policies generally place a prohibition on use of e-mails in a way that could be interpreted as offensive or harassing and specifically place a prohibition on viewing or sending any e-mail that could be viewed by a person as disparaging to any group, including those protected by title VII of the Civil Rights Act. These policies generally request that any employee who is aware of such a violation report the violation to either his manager or the human resources department. E-mail usage policies generally require that employees treat work-related e-mail as confidential information and for use or disclosure in the performance of job-related duties. Even more sophisticated companies place a restriction on forwarding e-mails, especially those that communicate with legal counsel (either external or internal), are of a legal nature, or could end up in a legal context or litigation. Further, these policies request that employees retain or include an attorney-client notation on e-mail that they receive from legal counsel or employees acting on behalf of their legal counsel in the context of a legal investigation or litigation. All of these restrictions set forth in common email policies should also be considered for instant messaging and text message communications.

§ 3.2:6 Retention of Electronic Communication Content

Computer usage policies should instruct employees to cease deletion of any electronic communication content, data, or documents that relate to any known claim, lawsuit, investigation, or audit that is ongoing or expected. Except for the documents of legal concern set forth in the prior sentence, computer usage policies require employees to retain documents for only the period prescribed by the DRP. Such policies also inform employees that documents and electronic communications properly stored on the appropriate servers will be deleted in accordance with the retention policies set forth by the company. Company DRPs should request that employees store electronic communications and documents only in designated locations, such as specific servers, and generally discourage saving such ESI in other locations. Compliance with this policy is important in the context of e-discovery, as the company may not be aware of relevant ESI, in the form of PST files or otherwise, that is directly relevant to a particular litigation, audit, or investigation.

§ 3.2:7 Treatment of Confidential Content

Computer usage policies should include a restriction against disclosure of confidential and proprietary information. Disclosure includes forwarding any content (by electronic means or otherwise) to third parties. Further, companies should include a provision that restricts employees from disclosure of personal identification and passwords.

§ 3.2:8 Personal or External Storage Devices

Computer usage policies should regulate the downloading of company data to employees' personal storage devices or other sites (for example, Dropbox or other cloud storage sites or remote backup services). In some contexts, third-party storage devices might make certain job functions more effective by allowing movement of projects between company-owned and employee-owned devices or between company-owned and customer-owned devices. Without regulating such devices or having certain guidelines followed, however, the company may find it difficult to respond to litigation hold notices that pertain to data stored on employee-owned devices.

§ 3.2:9 Explicit Use Policy

Companies should establish clear policies on the use of personal devices, including definitions regarding the use of the company network, devices located on company property, and when devices can be used in the normal course of business. An example of why an explicit use policy is necessary to limit liability is to prevent employees from using their personal devices to access websites with offensive or harassing content while engaged in regular business activities.

§ 3.2:10 Litigation Hold/Discovery Policy

It is vital for employees to identify the devices they have used to access, create, or modify company documents. This policy must make clear that if a personal device is used for business purposes, the employer has the right and may have an obligation to forensically preserve information used from that device. Additionally, employees must be informed and trained that deletion of company data from these devices during litigation holds will not be tolerated and severe consequences will be in place for violation of this policy.

§ 3.2:11 Terminated Employee Policy

One of the most overlooked policies relating to employee-owned devices and e-discovery covers preserving data from recently terminated employees. Companies can potentially mitigate or avoid sanctions by instituting a policy of forensically acquiring all devices that have accessed the corporate network as part of the termination process. There could be a fine line between the personal data and business data stored on such devices, so a thoughtful procedure should be developed and deployed to ensure that the company is not over-collecting data from the former employee's personal device, but is at the same time meeting its duties to preserve relevant data.

§ 3.2:12 White-Listing

A company can track devices connected to the company network via a method known as white-listing. Employees would be required to submit a request to the company network support team before being allowed to access their employer's secure network. The network support team would then allow access to the network for only the devices identified by the employee. A strict adherence to the white-listing procedure would create a log of all devices that have access to the network, assisting with proper scoping of ESI collections.

§ 3.2:13 VPN Policies

It is important to consider the ways in which devices can be used to connect to the network. One of the most common methods used to access a company network from a device that is not directly connected to the network is by using virtual private network (VPN) software. This software creates a secure connection between the device and the network. Proper VPN logging combined with white-listing can allow employees the flexibility to work from any location, while protecting company information, assets, and vulnerabilities.

§ 3.2:14 Password Policies

If an employee introduces a personally owned device into the company network via email or VPN, a company may require that the device meets minimum password complexity requirements. These policies must extend to all devices that interact with a company's network, regardless of ownership.

§ 3.3 Document Retention Policies (DRPs)

A DRP is an internal document that regulates the time frame documents (including ESI) that may be retained on the company's servers, hard drives, or other storage devices. The DRP is the nexus between and among the human resources (HR) department, the information technology (IT) department, and the legal department. The DRP also allows for exceptions in the case of litigation hold notices, at least to the extent that certain ESI may be reasonably within the scope of the litigation hold. A DRP should (1) reduce the cost of storage (by reducing ESI or limiting the continuous expansion of ESI stored on the company's systems or in the cloud); (2) ensure data that is no longer relevant to the company's business (that is, no longer useful from an operational or historical perspective) is deleted and similar data is not retained on a systematic basis in the future; (3) ensure that useful data is retained, properly placed, and stored in a location where information may be readily accessible by intended users; and (4) ensure that where data is stored makes sense from a data accessibility perspective. An effective DRP has the added benefit of reducing storage costs and

Computer Usage Policies

the subject of a discovery request.

§ 3.4

Key attributes of a successful and effective DRP include a policy that (1) protects important business information; (2) deletes unimportant or obsolete information; (3) trains employees on the rules of the policy so it may be effectively enforced; (4) encourages employees to enforce the rules; (5) encourages retention of final documents (that is, setting rules to delete prior drafts when applicable); (6) enables the HR department to work with the IT department to deploy rules; (7) sets a limited duration for saving voice mail messages; (8) permanently deletes documents without other ways to retrieve data once deleted; (9) covers all company-related documents created by employees and representatives of the company in furtherance of the business; (10) sets up processes that reflexively protect the deletion of documents that may be subject to any threatened or actual litigation, governmental investigation, or audit; and (11) schedules an annual audit of the DRP to confirm that it functions as prescribed in the DRP. If issues arise from an audit, such deficiencies should be addressed and corrected. If corrections are not workable, the company's management should reset rules of the DRP so that they are workable and can be complied with going forward.

§ 3.4 ESI and Duty to Preserve

Effective document retention policies assist companies dealing with the legal duty to preserve ESI when faced with a litigation hold notice. In the 1998 case *Kronisch v. United States*, the court identified when the duty to preserve ESI begins, stating that—

[The] obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation—most commonly when suit has already been filed, providing the party responsible for the destruction with express notice, but also on occasion in other circumstances, as for example when a party should have known that the evidence may be relevant to future litigation.²

Once the internal or external legal team has established that a duty to preserve exists, a party to litigation must determine the scope of ESI to be collected. In *Zubulake v. UBS Warburg LLC*, the court stated that—

while a litigant is under no duty to keep or retain every document in its possession . . . it is under a duty to preserve what it knows, or reasonably

^{2.} Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998).

should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.³

When proper accounting of company-owned devices is conducted (and, if relevant, in the BYOD context), a company can substantiate that its ESI collection activities were reasonable.

§ 3.5 Spoliation

Because the burden of preservation and production of all relevant ESI—regardless of the location—falls to the company, it is critical that organizations understand the consequences of failure to meet their discovery obligations. Spoliation has been broadly defined as the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation.⁴ Obstruction occurs when a person "influences, obstructs, or impedes, or endeavors to influence, obstruct, or impede, the due administration of justice."⁵

From a company's risk management and legal risk perspective, the risk of sanctions for failing to preserve relevant ESI should encourage companies to set up practices, policies, and systems that reduce the potential for such claims being brought against the company in future litigation.

§ 3.6 Responding to E-Discovery Requests

DRPs also allow for effective engagement with the party requesting documents or data in order to determine what is reasonably available and can be produced at a burden and cost that is proportional to the case. Pursuant to Fed. R. Civ. P. 26(f), the parties are required to meet and confer about e-discovery and to develop a plan for appropriate discovery of ESI. The party receiving the request (the responding party) should note that "[a] party need not provide discovery of ESI from sources that the party identifies as not reasonably accessible because of undue burden or cost."⁶ How-

^{3.} Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (quoting Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991)).

^{4.} See Richard Griffith & R. Jeffrey Layne, Spoliation of Evidence: Remedies and Implication, Texas Tech/St. Mary's Medical Malpractice Conference, 1 (April 1995); Steffen Nolte, The Spoliation Tort: An Approach to Underlying Principles, 26 St. Mary's L.J. 351, 361–64 (1995); Philip A. Lionberger, Interference with Prospective Civil Litigation by Spoliation of Evidence: Should Texas Adopt a New Tort, 21 St. Mary's L.J. 209, 219–23 (1989–1990).

^{5. 18} U.S.C. § 1503(a).

ever, the responding party must identify the sources it contends are not reasonably accessible and make a showing of undue burden or cost. Even if information is not reasonably accessible, "the court may nonetheless order discovery from such sources if the requesting party shows good cause."7 Data generally considered to be accessible is typically active data (that is, online and in use). Next in line is near-line data (for example, CDs or flash drives), then off-line archives (for example, indexed or organized tapes), then off-line storage (that is, hard copy documents), then erased or fragmented files (that is, deleted files), and then legacy data (that is, data that related to systems no longer in use). Further, the requesting party may, but is not required to, identify the form in which it wants the material produced. If the requesting party does not identify a form of production, or if the responding party objects to the form identified by the requesting party, the responding party must state its objection and identify the form in which it intends to produce.8 Generally the default format for ESI is the format in which it is ordinarily maintained and reasonably usable. In document-intensive cases, the parties often agree to a standard production format that includes a database load file with certain fielded information, such as author, recipient, date sent, etc.

§ 3.7 Using DRPs to Reduce Costs

Companies tend to accumulate increasing amounts of ESI because the cost of storing such data is continuously less expensive. The cost of e-discovery requests during litigation, investigations, or audits, however, can be quite substantial. The cost of attorney review of one gigabyte of data has been estimated to be \$18,000 or more.⁹

Companies that utilize a document retention policy and actively (but prudently) delete data that is not subject to a litigation hold and not required to be preserved can help reduce the amount of data that must be migrated to an e-discovery software platform and subsequently reviewed.

§ 3.8 Responding to Litigation Demands

Once a company receives a litigation hold letter, audit request, or investigative request, the legal department, acting in concert with the IT department, should

- 6. Fed. R. Civ. P. 26(b)(2)(B).
- 7. Fed. R. Civ. P. 26(b)(2)(B).
- 8. Fed. R. Civ. P. 26(b)(2)(D).

9. Nicholas M. Pace & Laura Zakaras, *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*, RAND Institute for Civil Justice (2012), www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1208.pdf, p. 21 fig. 2-2.

respond by fencing off specific areas where responsive ESI is held. Within the context of e-discovery, all ESI that may be responsive to the request should be retained, and any and all destruction of such ESI should be halted until such time as the request is no longer active. How well a company executes its fencing off of ESI will determine whether or not it will be able to successfully defend against a claim of spoliation and protect itself from unwanted inferences or sanctions.

A well-drafted DRP should flexibly respond to litigation and threats of litigation. Upon receipt of a demand letter requesting that the company cease destroying documents that may be related to anticipated litigation, the DRP should be looked to as a guidepost to the next steps relating to data or ESI.

Upon receipt of information that would cause a company to reasonably anticipate litigation, the company should promptly disseminate a litigation hold notice through the appropriate parts of the organization and fence off deletion activities that might affect relevant ESI.¹⁰ One area plaguing companies attempting to respond to litigation hold notice letters is how to treat transitory data. Transitory data is information that exists for a very brief, transitory period, often stored in RAM. An example of transitory data is a document that someone has deleted from a hard drive. The deletion of a document doesn't mean that it disappears; rather, the location of the document is identified as available to be written over when space is needed. Therefore, a DRP should address how it will deal with deletion of transitory data or temporary caches of data in the context of a litigation hold.¹¹

When particular individual hard drives house relevant data, mirror-imaging the hard drive is the best course of action rather than pulling specific data for preservation. A mirror image of the hard drive will defend against arguments of neglectful data preservation under either a litigation hold or a court order requiring the preservation of certain data. Arguments may be addressed as to irrelevant data housed on a particular hard drive from inside the company or from specific personnel who have been assigned the hard drive, but creating a mirror image does not mean that all data will be produced or, if it is produced in whole, that it will be disclosed without a protective order.

^{10.} See Pension Committee v. Banc of America, 685 F. Supp. 2d 456 (S.D.N.Y. 2010) (abrogated on other grounds by Chin v. Port Authority of New York & New Jersey, 685 F.3d 135, 162 (2d Cir. 2012)).

^{11.} Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 176 (S.D.N.Y. 2004).

§ 3.9 Conclusion

Within the context of e-discovery and litigation, records management and information governance policies and practices play an important role. A well-drafted DRP with clear terms, consistent deployment, and effective enforcement will serve a company or agency well in the midst of actual or threatened litigation, investigation, or audit. Alternatively, failure by a company to develop, deploy, and enforce a DRP may negatively impact the company by focusing its executives and lawyers on defensive issues like spoliation of data and sanctions, rather than strategic matters key to winning a case or defending claims made in an audit or investigation. A well-documented DRP can mean the difference between responding to litigation or an investigation in a proactive, offensive, effective, and strategic manner, or responding in a more reactive, defensive, ineffective, costly, and tact cal manner.



Chapter 4

Introduction to Digital Data, Computers, and Storage Media

Craig Ball

§ 4.1 Introduction

In 1774, a Swiss watchmaker named Pierre Jaquet-Droz built an ingenious mechanical doll resembling a barefoot boy. Constructed of six thousand handcrafted parts and dubbed "L'Ecrivain" ("The Writer"), Jaquet-Droz's automaton uses quill and ink to handwrite messages in cursive, up to forty letters long, with the content controlled by interchangeable cams. The Writer is a charming example of an early programmable computer.

The monarchs that marveled at Jaquet-Droz's little penman didn't need to understand how it worked to enjoy it. Lawyers, too, once had little need to understand the operation of their clients' information systems to conduct discovery. But the paper era is over, and digital reigns. Consider how much of our lives are lived online via digital devices! Think how much has been instrumented and networked! All of us are as telemetered today as the Apollo astronauts of fifty years ago. Never in human history has there been so much probative and reliable evidence for lawyers to draw on to help us draw closer to the truth. We are so lucky!

But as the volume of electronically stored information ("ESI") has exploded and the forms and sources of ESI continue to morph and multiply, lawyers conducting electronic discovery cannot ignore the watch works. New standards of competence demand that lawyers master some fundamentals of information technology and electronic evidence.

§ 4.2 Digital Data

Despite its daunting complexity, all digital content—photos, music, documents, spreadsheets, databases, social media, and communications—exist in one common and mind-boggling form. Almost all the information in the world exists on hard drives as faint electric charges or impossibly tiny reversals of magnetic polarity. These minute polar fluctuations are read by a detector flying above the surface of a spinning disk on a cushion of air one-thousandth the width of a human hair in an operation akin to a jet fighter flying around the world at more than eight hundred times the speed of sound less than a millimeter above the ground and precisely counting every blade of grass it passes!

That's astonishing, but what should astound you more is that there are no pages, paragraphs, spaces, or markers of any kind to define the data stream. That is, the history, knowledge, and creativity of humankind manifest as two different states (on/off . . . one/zero) in a continuous, featureless expanse. It's a data stream that carries not only the information we store but all the instructions needed to make sense of the data as well. It holds all the information about the data required to play it, display it, transmit it, or otherwise put it to work. It's a reductive feat that will make your head spin, and make you want to buy a computer scientist a drink.

Yet it should comfort you to know that no matter the volume or variety of digital electronic evidence, electronic evidence is more alike than different. E-discovery is rarely "push-button easy"; but it's far easier to preserve, collect, search, process, review, and produce once you see its common threads. That's why information technologists are prone to dismiss overblown claims of burden with the observation, "It's just data."

§ 4.2:1 Data, Not Documents

Lawyers—particularly those who didn't grow up with computers—tend to equate data with documents when, in a digital world, documents are just one variant of the many forms in which electronic information exists. Documents, like the letters, memos, and reports of yore, account for a miniscule share of electronically stored information relevant in discovery. Too, documents derived from electronic sources tend to convey just part of the information stored in the source. The decisive information in a case may exist as nothing more than a single bit of data that, in context, signals whether the fact you seek to establish is true or not. A Facebook page doesn't exist until a request sent to a database triggers the page's assembly and display. Word documents, PowerPoint presentations, and Excel spreadsheets lose content and functionality when printed to screen images or paper.

With so much discoverable information bearing so little resemblance to documents, and with electronic documents carrying much more probative and useful information than a printout or screen image conveys, competence in electronic discovery demands an appreciation of data more than documents.

§ 4.2:2 Binary

When we were children starting to count, we had to learn the decimal system. We had to think about what numbers meant. When our first-grade selves tackled a big number like 9,465, we were acutely aware that each digit represented a decimal multiple. The nine was in the thousands place, the four in the hundreds, the six in the tens place and so on. We might even have parsed 9,465 as $(9 \times 1000) + (4 \times 100) + (6 \times 10) + (5 \times 1)$.

But soon it became second nature to us. We'd unconsciously process 9,465 as nine thousand four hundred sixty-five. As we matured we learned about powers of ten and then saw 9,465 as $(9 \times 10^3) + (4 \times 10^2) + (6 \times 10^1) + (5 \times 10^0)$. This was exponential, or "base ten," notation.

Mankind probably uses base ten to count because we evolved with ten fingers. But, had we slithered from the ooze with eight or twelve digits, we'd have gotten on splendidly using a base eight or base twelve number system. It really wouldn't matter because any number—and consequently any data—can be expressed in any number system. So it happens that computers use the base two, or "binary," notation, and computer programmers are partial to base sixteen, or "hexadecimal," notation. It's all just counting. The radix, or base, is the number of unique digits, including the digit zero used to represent numbers in a positional numeral system. For example, in the decimal system, the radix is ten because it uses the ten digits from 0 through 9.

§ 4.2:3 Bits

Computers use binary digits in place of decimal digits. The word "bit" is even a shortening of the words "binary digit." Unlike the decimal system where any number is represented by some combination of ten possible digits (0–9), the bit has only two possible values: zero or one. This is not as limiting as one might expect when considering that a digital circuit—essentially an unfathomably complex array of switches hasn't got any fingers to count on, but is very good and very fast at being "on" or "off."

In the binary system, each binary digit—"bit"—holds the value of a power of two. Therefore, a binary number is composed of only zeroes and ones, like this: 10101. How do you figure out what the value of the binary number 10101 is? You do it in the same way we did it above for 9,465, but you use a base of two instead of a base of ten. Hence: $(1 \times 2^4) + (0 \times 2^3) + (1 \times 2^2) + (0 \times 2^1) + (1 \times 2^0) = 16 + 0 + 4 + 0 + 1 = 21$.

Moving from right to left, each bit you encounter represents the value of increasing powers of two, standing in for zero, two, four, eight, sixteen, thirty-two, sixty-four, and so on. That makes counting in binary easy. From 0 to 21, decimal and binary equivalents look like the Table 4-1.

DEC = BIN	DEC = BIN
0 = 00000	11 = 01011
1 = 00001	12 = 01100
2 = 00010	13 = 01101
3 = 00011	14 = 01110
4 = 00100	15 = 01111
5 = 00101	16 = 10000
6 = 00110	17 = 10001
7 = 00111	18 = 10010
8 = 01000	19 = 10011
9 = 01001	20 = 10100
10 = 01010	21 = 10101

Table 4-1: Decimal and binary equivalents

§ 4.2:4 Bytes

A byte is a sequence, or "string," of eight bits. The biggest number that can be stored as one byte of information is 11111111, equal to 255 in the decimal system. The smallest number is zero, or 00000000. Thus, there are 256 different numbers that can be stored as one byte of information. So what do you do if you need to store a number larger than 256? Simple! You use a second byte. This affords you all the combinations that can be achieved with sixteen bits, being the product of all the variations of the first byte and all of the second byte (256×256 , or 65,536). Using bytes to express values, any number that is greater than 256 needs at least two bytes to be expressed (called a "word" in geek speak), any number above 65,536 requires at least three bytes, and so on. A value greater than 16,777,216 (256^3 , or 224) needs four bytes (called a "long word"), and so on.

Let's try it: Suppose we want to represent the number 51,975. It's 1100101100000111.
(32768+16384+2048+512+256) or 51,968									- (4+2+1) or 7							
1	1	0	0	1	0	1	1	+	0	0	0	0	0	1	1	1
32768	16384	8192	4096	2048	1024	512	256		128	64	32	16	8	4	2	1
215	214	213	212	211	210	29	28		27	26	25	24	23	22	21	20

Table 4-2: Binary equivalent of 51,975

Why is an eight-bit sequence the fundamental building block of computing? It just sort of happened that way. In this time of cheap memory, expansive storage, and light-ning-fast processors, it's easy to forget how scarce and costly these resources were at the dawn of the computing era. Seven bits (with a leading bit reserved) was basically the smallest block of data that would suffice to represent the minimum complement of alphabetic characters, decimal digits, punctuation, and control instructions needed by the pioneers in computer engineering. It was, in another sense, about all the data early processors could chew on at a time, perhaps explaining the name "byte" (coined by IBM scientist Dr. Werner Buchholz in 1956).

§ 4.2:5 The Magic Decoder Ring Called ASCII

Back in 1935, American kids who listened to the *Little Orphan Annie* radio show (and who drank lots of Ovaltine) could join the Radio Orphan Annie Secret Society and obtain a Magic Decoder Ring with rotating disks that allowed them to write secret messages in numeric code.

Similarly, computers encode words as numbers. Binary data stand in for the uppercase and lowercase English alphabet, as well as punctuation marks, special characters, and machine instructions (like carriage return and line feed). The most widely deployed U.S. encoding mechanism is known as the ASCII code (for American Standard Code for Information Interchange, pronounced "ask-key"). By limiting the earliest ASCII character set to just 128 characters, any character can be expressed in just seven bits (2⁷, or 128) and so occupies less than one byte in the computer's storage and memory. In table 4-3 below, the columns reflect a binary (byte) value, its decimal equivalent, and the corresponding ASCII text value (including some for machine codes and punctuation):

8	4	2
3	-	-

Binary	Decimal	Character	Binary	Decimal	Character	Binary	Decimal	Character
00000000	000	NUL	00101011	043	+	01010110	086	V
00000001	001	SOH	00101100	044	,	01010111	087	w
00000010	002	STX	00101101	045	-	01011000	088	x
00000011	003	ETX	00101110	046		01011001	089	Y
00000100	004	EOT	00101111	047	1	01011010	090	Z
00000101	005	ENQ	00110000	048	0	01011011	091	ſ
00000110	006	ACK	00110001	049	1	01011100	092	N
00000111	007	BEL	00110010	050	2	01011101	093]
00001000	008	BS	00110011	051	3	01011110	094	۸
00001001	009	HT	00110100	052	4	01011111	095	-
00001010	010	LF	00110101	053	5	01100000	096	
00001011	011	VT	00110110	054	6	01100001	097	a
00001100	012	FF	00110111	055	7	01100010	098	b
00001101	013	CR	00111000	056	8	01100011	099	с
00001110	014	SO	00111001	057	9	01100100	100	d
00001111	015	SI	00111010	058	:	01100101	101	e
00010000	016	DLE	00111011	059		01100110	102	f
00010001	017	DC1	00111100	060	<	01100111	103	g
00010010	018	DC2	00111101	061	=	01101000	104	h
00010011	019	DC3	00111110	062	>	01101001	105	i
00010100	020	DC4	00111111	063	?	01101010	106	j
00010101	021	NAK	01000000	064	@	01101011	107	k
00010110	022	SYN	01000001	065	A	01101100	108	1
00010111	023	ETB	01000010	066	В	01101101	109	m
00011000	024	CAN	01000011	067	с	01101110	110	n
00011001	025	EM	01000100	068	D	01101111	111	0
00011010	026	SUB	01000101	069	E	01110000	112	p
00011011	02.7	ESC	01000110	070	F	01110001	113	q
00011100	028	FS	01000111	071	G	01110010	114	r
00011101	029	GS	01001000	072	Н	01110011	115	8
00011110	030	RS	01001001	073	I	01110100	116	t
00011111	031	US	01001010	074	J	01110101	117	u
00100000	032	SP	01001011	075	K	01110110	118	v
00100001	033	1	01001100	076	L	01110111	119	w
00100010	034	el	01001101	077	М	01111000	120	x
00100011	035	#	01001110	078	N	01111001	121	у
00100100	036	\$	01001111	079	0	01111010	122	z
00100101	037	%	01010000	080	р	01111011	123	{
00100110	038	&	01010001	081	Q	01111100	124	1
00100111	039	1	01010010	082	R	01111101	125	}
00101000	040	(01010011	083	S	01111110	126	~
00101001	041)	01010100	084	T	01111111	127	DEL
00101010	042	*	01010101	085	U		-	-

Table 4-3: ASCII table

So "E-Discovery" would be written in a binary ASCII sequence as:

It would be tough to remember your own name written in this manner! *Hi, I'm Craig, but my friends call me* **01000011**01110010**01100001**01101001**01100111**.

Note that each leading bit of each byte in Table 4-3 is a zero. It isn't used to convey any encoding information; that is, they are all 7-bit bytes. In time, the eighth bit (the leading zero) came to be used to encode another 128 characters (2⁸, or 256), leading to various "extended" (or "high") ASCII sets that include, for example, accented characters used in foreign languages and line drawing characters.

Unfortunately these extra characters weren't assigned in the same way by all computer systems. The emergence of different sets of characters mapped to the same high byte values prompted a need to identify these various character encodings or, as they are called in Windows, "code pages." If an application used the wrong code page, information would be displayed as gibberish. This is such a familiar phenomenon that it has its own name, "mojibake" (roughly translated from Japanese for "character changing"). If you've ever seen a bunch of Asian characters in an e-mail or document that you know was written in English, you might have glimpsed mojibake.

Note that we are speaking here of textual information, not typography, so don't confuse character encodings with fonts. The former tells you whether the character is an A or b, not whether to display the character in Arial or Baskerville typeface.

In the mid-1980s international standards began to emerge for character encoding, ultimately resulting in various code sets issued by the International Standards Organization (ISO). These retained the first 128 American ASCII values and assigned the upper 128 byte values to characters suited to various languages (e.g., Cyrillic, Greek, Arabic, and Hebrew). These various character sets were called ISO-8859-n, where the "n" distinguished the sets for different languages. ISO-8859-1 was the set suited to Latin-derived alphabets (like English), and so the most familiar code page to U.S. computer users came to be called "Latin 1."

However, Microsoft adopted the Windows code page before the ISO standard became final, basing its Latin 1 encoding on an earlier draft promulgated by the American National Standards Institute (ANSI). Thus, the standard Windows Latin-1 code page,

called Windows-1252 (ANSI), is *mostly* identical to ISO-8859-1, and it's common to see the two referred to interchangeably as "Latin 1."

§ 4.2:6 Unicode

ASCII was introduced in the pre-Internet world of 1963—before the world was flat, when the West dominated commerce, and personal computing was the stuff of science fiction. Using a single byte (even with various code pages) supported only 256 characters, so remained unsuited for Asian languages like Chinese, Japanese, and Korean, which employ thousands of pictograms and ideograms.

Though various ad hoc approaches to foreign language encodings were developed, a universal, systematic encoding mechanism was needed to serve an increasingly interconnected world. These methods used more than one byte to represent each character. The most widely adopted such system is called Unicode. In its latest incarnation (version 6.2) Unicode standardizes the encoding of one hundred written languages called "scripts" comprising 110,182 characters.

Unicode was designed to coexist with the longstanding ASCII and ANSI character sets by emulating the ASCII character set in corresponding byte values within the more extensible Unicode counterpart, UTF-8. Because of its backward compatibility and multilingual adaptability, UTF-8 has become a widely used encoding standard, especially on the Internet and within e-mail systems.

§ 4.2:7 Mind the Gap!

Now, as we talk about these bytes and encoding standards as a precursor to hexadecimal notation, it will be helpful to revisit how this all fits together. A byte is eight ones or zeroes, which means a byte can represent 256 different decimal numbers from 0–255. So two bytes can represent a much bigger range of decimal values (256×256 , or 65,536). Character encodings (a.k.a. "code pages") like Latin 1 and UTF-8 are ways to map textual, graphical, or machine instructions to numeric values expressed as bytes, enabling machines to store and communicate information in human languages. As we move forward, keep in mind that hex, like binary and decimal, is just another way to write numbers. Hex is not a code page, although the numeric values it represents may correspond to values within code pages.

§ 4.2:8 Hex

Long sequences of ones and zeroes are very confusing for people, so hexadecimal notation emerged as more accessible shorthand for binary sequences. Considering the prior discussion of base 10 (decimal) and base 2 (binary) notation, it might be enough to say that hexadecimal is base 16. In hexadecimal notation ("hex" for short), each digit can be any value from zero to fifteen. Accordingly, four binary digits can be replaced by just one hexadecimal digit, and more to the point, a byte can be expressed as just two hex characters.

The decimal system supplies only ten symbols (0-9) to represent numbers. Hexadecimal notation demands sixteen symbols, leaving us without enough single character numeric values to stand in for all the values in each column. So how do we cram sixteen values into each column? The solution is to substitute the letters A through F for the numbers 10 through 15. So we car represent 10110101 (the decimal number 181) as "B5" in hexadecimal notation. Using hex we can notate values from 0–255 as 00 to FF (using either lowercase or uppercase letters, it doesn't matter).

It's hard to tell if a number is decimal or hexadecimal just by looking at it. If you see "37," does that equate to 37 ("37" in decimal) or a decimal 55 ("37" in hexadecimal)? To get around this problem, two common notations are used to indicate hexadecimal numbers. The first is the suffix of a lowercase "h." The second is the prefix "0x." So "37 in hexadecimal," "37h," and "0x37" all mean the same thing.

Figure 4-1 below can be used to express ASCII characters in hex. The capital letter "G" has the hex value of 47 (i.e., row 4, column 7), so "E-Discovery" in hex encodes as:

0x 45 2D 44 69 73 63 6F 76 65 72 79, and that's easier than

0100010100101101**01000100**01101001**01110011**01100011**01101110**11101100**1100 101**01110010**01111001**.

1	0	11	12	13	14	1 5	6	17	18	9	1 A	B	C	D	E	F
	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	S0	SI
	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
		!	u	#	\$	%	&		()	*	+	,	-	•	1
	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
	0	A	B	C	D	E	F	G	H	I	J	К	L	M	N	0
	Ρ	Q	R	S	Т	U	۷	W	X	Y	Z]	1]	^	-
	•	a	b	С	d	e	f	g	h	i	j	k	ι	m	n	0
	р	q	r	s	t	u	V	W	x	У	Z	{	1	}	~	DEL

Figure 4-1: ASCII code chart

ASCTT Code Chant

The critical takeaway from all this is that ESI is just data, and data are just numbers that encode text, pixels, and geolocation data. Because numbers are easily altered, authenticity and admissibility of modern evidence hinges on whether we can trust those numbers—a trust contingent on the caliber of our tools and our skill using them.

Now that you have some sense of how information is encoded digitally, let's take a look at the media and devices that store and use digital data.

§ 4.3 Introduction to Data Storage Media

Mankind has been storing data for thousands of years—on stone, bone, clay, wood, metal, glass, skin, papyrus, paper, plastic, and film. In fact, people were storing data in binary formats long before the emergence of modern digital computers. Records from ninth century Persia describe an organ playing interchangeable cylinders. Eighteenth-century textile manufacturers employed perforated rolls of paper to control Jacquard looms, and Swiss and German music box makers used metal drums or platters to store tunes. At the dawn of the Jazz Age, no self-respecting American family of means lacked a player piano capable (more or less) of reproducing the works of the world's greatest pianists. Whether you store data as a perforation or a pin, you're storing binary data. That is, there are two data states: hole or no hole, pin or no pin, one or zero.

§ 4.3:1 Punched Cards

In 1889, U.S. inventor Herman Hollerith (1860–1929) was granted a patent for his system for storing data on perforated paper cards that revolutionized the 1890 U.S. census.¹ In the 1930s, demand for electronic data storage led to widespread adoption of Hollerith cards as a fast, practical, and cost-effective binary storage media. These

punched cards, initially made in a variety of sizes and formats, were ultimately standardized by IBM as the eighty-column, twelve-row (7.375" by 3.25") format below that dominated computing well into the 1970s. In the mid-1950s, punched card sales accounted for twenty percent of IBM's revenues. From 1975 to 1979, this author spent many a night in the basement of a computer center at Rice University typing program instructions onto these unforgiving punched cards, cousins to the oily, yellow perforated paper tape that Bill Gates and this author used on opposite coasts to program mainframe computers via a teletype terminal in the early 1970s.

Figure 4-2: IBM 5081 80-column card



The encoding schemes of these obsolete media differ from those we use today principally in speed and scale. The binary fundamentals are still fundamental and connect our toil in e-discovery and computer forensics to the likes of Charles Babbage, Alan Turing, Ada Lovelace, John von Neumann, Robert Noyce, and both Steves (Wozniak and Jobs). In the space of one generation, we have come extremely far indeed.

The IBM punched cards held eighty columns of twelve punch positions, or 960 bits. Nominally, that's 120 bytes, but because eight columns weren't always used for data storage, the storage capacity was closer to 864 bits, or 108 bytes—but not that much

^{1.} Hollerith founded The Tabulating Machine Company based in Georgetown, Washington, D.C. Hollerith's company was later merged with others and renamed International Business Machines Company, now IBM.

in fact because each column was typically dedicated to just one 7- or 8-bit ASCII character, so the practical capacity of a punched card was eighty characters/eighty bytes, or less.²

Using the 108-byte value, the formatted 1.44-megabyte, 3.5-inch floppy disks commonly used from the mid-1980s to early 2000s held 1,474,560 bytes, so a floppy disk could store the same amount of data as about 13,653 IBM punched cards; that is, seven 2,000-card boxes of cards or, at 143 cards to the inch, an eight-foot stack. That's a common ceiling height and taller than anyone who ever played in the NBA.

Fast-forward to today's capacious hard drives, a fifty-dollar terabyte drive holds 1,099,511,627,776 bytes. That's over *ten billion* IBM cards (10,180,663,220, to be precise). Now our stack of cards is 1,123 *miles*, or roughly the driving distance between Washington, D.C., and New Orleans. The 30-terabyte (compressed) capacity of an LTO-8 backup tape cartridge equals something like 305 billion IBM cards—a stack spanning 33,709 miles that would easily circle the globe at the Equator. See Figure 4-3 below.





These are hypothetical extrapolations, not real-world metrics, because much storage capacity is lost to file system overhead. If you used a warehouse for physical storage, you'd need to sacrifice space for shelving and aisles, and you'd likely find that not

^{2.} After hours researching the capacity question, I couldn't arrive at a definitive answer because capacity varied according to, among other things, the type of information being stored (binary versus ASCII) and a reluctance to punch out too many adjacent perforations lest it become a "lace card" too fragile to use.

everything you store perfectly fits wall-to-wall and floor-to-ceiling. Similarly, digital storage sacrifices capacity for file tables and wastes space by using fixed cluster sizes. If a file is smaller than the clusters allocated to its storage, then the bytes between the end of the file and the end of the cluster is wasted "slack space."

The 1950s saw the emergence of electromagnetic storage as the dominant medium for electronic data storage. Although solid-state storage will ultimately eclipse electromagnetic media for local storage, electromagnetic storage will continue to dominate network and cloud storage well into the 2020s, if not beyond.

§ 4.3:2 Magnetic Tape

The earliest popular form of electromagnetic data storage was magnetic tape. Compact cassette tape was the earliest data storage medium for personal computers, including the pioneering Radio Shack TRS-80 and the very first IBM personal computer, the model XT.

Spinning reels of tape were a clichéd visual metaphor for computing in films and television shows from the 1950s through the 1970s. Though the miles of tape on those reels now resides in cartridges and cassettes, tapes remain an enduring medium for backing up and archiving electronically stored information.

The LTO-8 format tapes introduced in 2017 house 3,150 feet of half-inch tape in a cartridge just four square inches and less than an inch thick, yet each cartridge natively holds twelve terabytes of uncompressed data and up to thirty terabytes of compressed data³ delivered at a transfer rate of 360 megabytes per second. LTO tapes use a back-and-forth, or "linear serpentine," recording scheme. "Linear" because it stores data in parallel tracks running the length of the tape, and "serpentine" because its path snakes back and forth, reversing direction on each pass. Thirty-two of the LTO-8 cartridge's 3,584 tracks are read or written as the tape moves past the recording heads, so it takes 112 back-and-forth passes, or "wraps," to read or write the full contents of a single LTO-8 cartridge.

That's sixty-seven miles of tape passing the heads, so it takes hours to read or write each tape—more than nine hours to write a full tape at maximum uncompressed speed. While tape isn't as fast as hard drives, it's proven to be more durable and less costly for long-term storage—as long as the data is being *stored*, not *restored*.

^{3.} Since most data stored on backup tape is compressed, the actual volume of ESI on tape may be more than twice greater than the native capacity of the tape.



Figure 4-4: Types of storage tape

§ 4.3:3 Floppy Disks

Today, the only place a computer user is likely to see a floppy disk is as the menu icon for storage on the menu bar of Microsoft Office applications. But floppy disks played a central role in software distribution and data storage for personal computing for thirty years.

Floppy disks are another form of electromagnetic storage. All floppy disks have a spinning, flexible plastic disk coated with a magnetic oxide (i.e., rust). The disk is essentially the same composition as magnetic tape in disk form. Disks were "formatted" (either by the user or pre-formatted by the manufacturer) to divide the disk into various concentric rings of data called "tracks," with tracks further subdivided into tiny arcs called "sectors." Formatting enables systems to locate data on physical storage media much as streets and house numbers enable us to locate homes in a neighborhood.

Figure 4-5: Types of disks



8" Floppy Disk in Use



Though many competing floppy disk sizes and formats have been introduced since 1971, only five formats are likely to be encountered in e-discovery. These are the 8-inch, 5.25-inch, 3.5-inch standard, and 3.5-inch high density and Zip formats. Of these, the 3.5HD format, 1.44 megabyte capacity floppy is by far the most prevalent legacy floppy disk format.

The Zip disk was one of several proprietary "super floppy" products that enjoyed brief success before the high capacity and low cost of recordable optical media (CD-R and DVD-R) and flash drives rendered them obsolete.

§ 4.3:4 Optical Media

The most common forms of optical media for data storage are the CD, DVD, and Bluray disks in read-only, recordable, or rewritable formats. Each typically exists as a 4.75-inch plastic disk with a metalized reflective coating and/or dye layer that can be distorted by a focused laser beam to induce pits and lands in the media. These pits and lands, in turn, interrupt a laser reflected off the surface of the disk to generate the 1s and 0s of digital data storage. The practical difference between the three prevailing forms of optical media are their native data storage capacities and the speed ("throughput") at which they can deliver data. In contrast to tape floppies and mechanical hard drives, optical storage media do not use electromagnetism to store and retrieve data.

A CD (for Compact Disk) or CD-ROM (for CD Read-Only Media) is read-only and not recordable by the end user. It's typically fabricated in factory to carry music or software. A CD-R is recordable by the end user, but once a recording session is closed it cannot be altered in normal use. A CD-RW is a re-recordable format that can be erased and written to multple times. The native data storage capacity of a standardsize CD is about 700 megabytes.

A DVD (for Digital Versitile Disk) also comes in read-only, recordable (DVD-R) and rewritable (DVD-RW) iterations, and the most common form of the disk has a native data storage capacity of approximately 4.7 gigabytes. So one DVD holds the same amount of data as six and one-half CDs.

By employing the narrower wavelength of a blue laser to read and write disks, a dual layer Blu-ray disk can hold up to about fifty gigabytes of data, equaling the capacity of about ten and one-half DVDs. Like their predecessors, Blu-ray disks are available in recordable (BD-R) and rewritable (CD-RE) formats.

Though ESI resides on a dizzying array of media and devices, by far the largest complement of same occurs within three closely related species of computing hardware: computers, hard drives, and servers. A server is essentially a computer dedicated to a specialized task or tasks, and both servers and computers routinely employ hard drives for program and data storage.

§ 4.3:5 Electromagnetic Hard Drives

As noted, mankind has long stored information by translating it into physical manifestations: cave drawings, Gutenberg bibles, musical notes, Braille dots, or undulating grooves on a phonograph record. Because it's simply a long sequence of 1s and 0s, binary data can be recorded by any number of physical phenomena. You could build a computer that stored data as a row of beads (the abacus), holes punched in paper (a piano roll), black and white vertical lines (bar codes), or bottles of beer on the wall (still waiting for this one!). If we build our computer to store data using bottles of beer on the wall, we'd better be plenty thirsty because we will need lots of beer bottles to get up and running. And we will need time to set up the bottles up, count them, and replace them as data changes. Too, we will need something like the Great Wall of China to hold them. So our beer bottle data storage system isn't practical. Instead, we need something compact, lightweight, and efficient—in short, a refrigerator magnet and some paper clips.

Maybe not a refrigerator magnet per se, but the principles are the same. If you take a magnet off your refrigerator and rub it against a metal paperclip, you will transfer some magnetic properties to the paperclip. Suppose you lined up about a zillion paper clips and magnetized some but not others. You could go down the row with a piece of ferrous metal (or better yet, a compass) and distinguish the magnetized clips from the non-magnetized clips. If you call the magnetized clips "1s" and the non-magnetized clips "0s," you've got yourself a system that can record binary data. Were you to glue all those paper clips in concentric circles onto a spinning phonograph record and substitute an electromagnet for the refrigerator magnet, you wouldn't be too far afield of what goes on inside the disk drives of a computer, albeit at a much smaller scale. In case you wondered, this is also how sound on magnetized as it rolls by, we gauge varying degrees of magnetism that correspond to variations in the recorded sounds. This is analog recording—the variations in the recording are analogous to the variations in the music.

Since computers process electrical signals much more effectively than they process magnetized paper clips jumping onto a knife blade, what is needed is a device that transforms magnetic signals to electrical signals and vice-versa—an energy converter. Inside every floppy and hard disk drive is a gadget called a read/write head. The read/ write head is a tiny electromagnet that perform the conversion from electrical information to magnetic and back again. Each bit of data is written to the disk using an encoding method that translates 0s and 1s into patterns of magnetic flux reversals. Don't be put off by Star Wars lingo like "magnetic flux reversal"—it just means flipping the magnet around to the other side, or "pole."

Older hard disk heads make use of the two main principles of electromagnetic force. The first is that an electrical current passed through a coil produces a magnetic field; this is used when writing to the disk. The direction of the produced magnetic field depends on the direction that the current is flowing through the coil. The converse principle is that a magnetic field applied to a coil will cause an electrical current to flow, which is useful for reading back previously written information. Newer disk heads use different physics and are more efficient, but the basic approach hasn't changed: electricity to magnetism and magnetism to electricity.

A hard drive is an immensely complex data storage device that's engineered to appear deceptively simple. When you connect a hard drive to your machine, the operating system detects the drive, assigns it a drive letter, and—presto!—you've got trillions of bytes of new storage! Microprocessor chips garner the glory, but the humdrum hard drive is every bit a paragon of ingenuity and technical prowess.

A conventional personal computer hard drive is a sealed aluminum box measuring (for a desktop system) roughly $4" \times 6" \times 1"$ in height. A hard drive can be located almost anywhere within the case and is customarily secured by several screws attached to any of ten pre-threaded mounting holes along the edges and base of the case. One face of the case will be labeled to reflect the drive specifications, while a printed circuit board containing logic and controller circuits will cover the opposite face.

A conventional hard disk contains round, flat disks called "platters" coated on both sides with a special material able to store data as magnetic patterns. Much like a record player, the platters have a hole in the center allowing multiple platters to be stacked on a spindle for greater storage capacity.

The platters rotate at high speed—typically 5,400, 7,200, or 10,000 rotations per minute—driven by an electric motor. Data is written to and read from the platters by tiny devices called "read/write heads" mounted on the end of a pivoting extension called an "actuator arm" that functions similarly to the tone arm that carried the phonograph cartridge and needle across the face of a record. Each platter has two read/write heads, one on the top of the platter and one on the bottom. So a conventional hard disk with three platters typically sports six surfaces and six read/write heads.

Unlike a record player, the read/write head never touches the spinning platter. Instead, when the platters spin up to operating speed, their rapid rotation causes air to flow under the read/write heads and lift them off the surface of the disk—the same principle of lift that operates on aircraft wings and enables the aircraft to fly. The head then reads the magnetic patterns on the disk while flying just a half millionth of an inch above the surface. At this speed, if the head bounces against the surface, there is a good chance that the head will burrow into the surface of the disk, obliterating data, destroying both read/write heads, and rendering the hard drive inoperable—a so-called "head crash."



Figure 4-6: Conventional personal computer hard drive

The hard disk drive has been around for more than fifty years, but it was not until the 1980s that the physical size and cost of hard drives fell sufficiently for their use to be commonplace.

Introduced in 1956, the IBM 350 Disk Storage Unit was the first commercial hard drive. It was sixty inches long, sixty-eight inches high, and twenty-nine inches deep

(so it could fit through a door). Called the RAMAC (for Random Access Method of Accounting and Control), it held fifty 24-inch magnetic disks of fifty thousand sectors, each storing one hundred alphanumeric (7-bit) characters. Thus, it held about 3.75 megabytes, or one or two cell phone snapshots today. It weighed a ton (literally), and users paid \$3,200 per month to rent it. That's about \$30,000 in today's dollars.

Now you can buy a 10-terabyte hard drive storing *two million times* more information for a fraction of that monthly rental That 10-terabyte drive weighs less than two pounds, can hide behind a paperback book, and costs \$250.

Over time, hard drives took various shapes and sizes (or "form factors," as the standard dimensions of key system components are called in geek speak). Three form factors are still in use: 3.5" (desktop drive), 2.5" (laptop drive), and 1.8" (iPod and microsystem drive, now supplanted by solid-state storage).

Hard drives connect to computers by various mechanisms called "interfaces" that describe both how devices "talk" to one another as well as the physical plugs and cabling required. The five most common hard drive interfaces in use today are:

- 1. PATA, for parallel advanced technology attachment (sometimes called EIDE for extended integrated drive electronics);
- 2. SATA, for serial advanced technology attachment;
- 3. SCSI, for small computer system interface;
- 4. SAS, for serial attached SCSI; and
- 5. FC, for fibre channel.

Figure 4-7: PATA and SATA hard drive interfaces



Though once dominant in personal computers, PATA drives largely disappeared in 2006. Today, virtually all laptop and desktop computers employ SATA drives for local storage. SCSI, SAS, and FC drives tend to be seen exclusively in servers and other applications demanding high performance and reliability.

From the user's perspective, PATA, SATA, SCSI, SAS, and FC drives are indistinguishable; however, from the point of view of the technician tasked to connect to and image the contents of the drive, the difference implicates different tools and connectors.

The five drive interfaces divide into two employing parallel data paths (PATA and SCSI) and three employing serial data paths (SATA, SAS, and FC). Parallel ATA interfaces route data over multiple simultaneous channels necessitating forty wires, where serial ATA interfaces route data through a single high-speed data channel requiring only seven wires. Accordingly, SATA cabling and connectors are smaller than their PATA counterparts.

Fibre Channel (FC) employs optical fiber (the spelling difference is intentional) and light waves to carry data at impressive speeds. The premium hardware required by FC dictates that it will be found in enterprise computing environments, typically in conjunction with a high-capacity/high-demand storage device called a SAN (for storage attached network) or a NAS (for network attached storage).

It's easy to become confused between hard drive interfaces and external data transfer interfaces like USB or FireWire seen on external hard drives. The drive within the external hard drive housing will employ one of the interfaces described above (except FC); however, to facilitate external connection to a computer, a device called a "bridge" will convert data written to and from the drive to a form that can traverse a USB or FireWire connection. In some compact, low-cost external drives, manufacturers dispense with the external bridge board altogether and build the USB interface right on the hard drive's circuit board.

§ 4.3:6 Flash Drives, Memory Cards, SIMs, and Solid-State Drives

Computer memory storage devices have no moving parts and the data resides entirely within the solid materials that compose the memory chips, hence the term "solid state." Historically, rewritable memory was volatile (in the sense that contents disappeared when power was withdrawn) and expensive. But beginning around 1995, a type of nonvolatile memory called "NAND flash" became sufficiently affordable to be used for removable storage in emerging applications like digital photography. Further leaps in the capacity and dips in the cost of NAND flash led to the near-eradication of film for photography and the extinction of the floppy disk, replaced by simple, inexpensive, and reusable USB storage devices called, variously, SmartMedia flash memory, CompactFlash flash memory, SD cards, flash drives, thumb drives, pen drives, and memory sticks or keys.

A specialized form of solid-state memory seen in cell phones is the subscriber identification module, or SIM card. SIM cards serve both to authenticate and identify a communications device on a cellular network and to store SMS messages and phone book contacts.



Figure 4-8: Types of removable storage drives

As the storage capacity of NAND flash has gone up and its cost has come down, the conventional electromagnetic hard drive is rapidly being replaced by solid-state drives in standard hard drive form factors. Solid-state drives are significantly faster, lighter, and more energy-efficient than conventional drives, but they currently cost anywhere from ten to twenty times more per gigabyte than their mechanical counterparts. All signs point to the ultimate obsolescence of mechanical drives by solid-state drives, and some products (notably tablets like the iPad and Microsoft Surface, as well as premium laptops) have eliminated hard drives altogether in favor of solid-state storage.

Currently, solid-state drives assume the size and shape of mechanical drives to facilitate compatibility with existing devices. However, the size and shape of mechanical hard drives were driven by the size and operation of the platter they contain. Because solid-state storage devices have no moving parts, they can assume virtually any shape. It's likely, then, that slavish adherence to 2.5-inch and 3.5-inch rectangular form factors will diminish in favor of shapes and sizes uniquely suited to the devices that employ them.

With respect to e-discovery, the shift from electromagnetic to solid-state drives is inconsequential. However, the move to solid-state drives will significantly impact matters necessitating computer forensic analysis. Because the NAND memory cells that comprise solid state drives wear out rapidly with use, solid state drive controllers must constantly reposition data to ensure usage is distributed across all cells. Such "wear leveling" hampers techniques that forensic examiners have long employed to recover deleted data from conventional hard drives.

§ 4.3:7 RAID Arrays

Whether local to a user or in the cloud, hard drives account for nearly all the electronically stored information attendant to e-discovery. In network server and cloud applications, hard drives rarely work alone. That is, hard drives are ganged together to achieve greater capacity, speed, and reliability in so-called "redundant arrays of independent disks," or RAIDs. In certain SANs, hard drives housed in trays may be accessed as Just a Bunch of Disks, or JBOD, but it's far more likely they are working together as a RAID.

RAIDs serve two ends: redundancy and performance. The redundancy aspect is obvious—two drives holding identical data safeguard against data loss due to mechanical failure of either drive—but how do multiple drives improve performance? The answer lies in splitting the data across more than one drive using a technique called "striping."

A RAID improves performance by dividing data across more than one physical drive. The swath of data deposited on one drive in an array before moving to the next drive is called the "stripe." If you imagine the drives lined up alongside one another, you can see why moving back and forth across the drives to store data might seem like painting a stripe across the drives. By striping data, each drive can deliver their share of the data simultaneously, increasing the amount of information handed off to the computer's microprocessor.

But when you stripe data across drives, information is lost if any drive in the stripe fails. You gain performance but surrender security.

This type of RAID configuration is called a "RAID 0." It wrings maximum performance from a storage system, but it's risky. If RAID 0 is for gamblers, "RAID 1" is for the risk-averse. A RAID 1 configuration duplicates everything from one drive to an identical twin, so that a failure of one drive won't lead to data loss. RAID 1 doesn't improve performance, and it requires twice the hardware to store the same information.

Other RAID configurations strive to integrate the *performance* of RAID 0 and the protection of RAID 1.

Thus, a "RAID 0+1" mirrors two striped drives but demands four hard drives, delivering only half their total storage capacity. Safe and fast, but not cost-efficient. The solution lies in a concept called "parity," key to a range of other sequentially numbered RAID configurations. Of those other configurations, the ones most often seen are called RAID 5 and RAID 7.

To understand parity, consider the simple equation 5 + 2 = 7. If you didn't know one of the three values in this equation, you could easily solve for the missing value; for example, presented with " $5 + _ = 7$," you can reliably calculate the missing value is 2. In this example, "7" is the "parity value," or checksum, for "5" and "2."

The same process is used in RAID configurations to gain increased performance by striping data across multiple drives while using parity values to permit the calculation of any missing values lost to drive failure. In a three-drive array, any one of the drives can fail, and we can use the remaining two to recreate the third (just as we solved for 2 in the equation above).





In Figure 4-9, data is striped across three hard drives, HDA, HDB, and HDC. HDC holds the parity values for data stripe 1 on HDA and stripe 2 on HDB. It's shown as "Parity (1, 2)." The parity values for the other stripes are distributed on the other

drives. Again, any one of the three drives can fail and all of the data is recoverable. This configuration is RAID 5 and, though it requires a minimum of three drives, it can be expanded to dozens or hundreds of disks.

§ 4.3:8 Hashing Data

Because all digital data is numbers, the arithmetic around parity values helps guard against data loss. More advanced math called "hashing" makes it possible to authenticate, deduplicate, and cull digital data. Hashing is the use of mathematical algorithms to calculate a unique sequence of letters and numbers to serve as a reliable digital "fingerprint" for electronic data. These sequences are called "message digests," or, more commonly, "hash values."⁴ It's an invaluable tool in both computer forensics and electronic discovery, and one deployed by courts with growing frequency.⁵

Using hash algorithms, any amount of data—from a tiny file to the contents of entire hard drives and beyond—can be expressed as an alphanumeric sequence of fixed length. The most common forms of hashing are MD5 and SHA-1. MD5 is a 128-bit (16-byte) value that is typically expressed as 32 hexadecimal (Base16) characters.

A hash value is just a big number calculated on the contents of the file. A 128-bit number can be as large as 2^{128} —if you start doing the $2 \times 2 \times 2 \times 2$ and so forth, you'll see how fast the values mount.

To say 128 bits or 2¹²⁸ is "big" doesn't begin to convey its unfathomable, astronomic scale. In decimal terms, it's about 340 billion billion billion billion, or 340 undecillion. That's four quadrillion times the number of stars in the observable universe! A SHA-1 hash value is an even larger 160-bit (20-byte) value that is typically expressed as 40-hex characters. So a SHA-1 value is an even bigger number—4.3 billion times bigger.

The MD5 hash value of the plain text of Lincoln's Gettysburg Address is E7753A4E97B962B36F0B2A7C0D0DB8E8. Anyone anywhere performing the same hash calculation on the same data will get the same unique value in a fraction of a second. But change the words in the speech from "Four score and seven" to "Five

^{4.} Refrain from saying "hash marks" unless you are speaking of insignia denoting military rank or the yard markers on a football field. The one-way cryptographic calculations used to digitally fingerprint blocks of data are "hash values," "hashes," or "message digests."

^{5.} In 2017, Federal Rule of Evidence 902 was amended to support self-authentication of digital evidence when supported by a process of digital identification like hashing. Fed. R. Evid. 902(14).

score," and the hash becomes 8A5EF7E9186DCD9CF618343ECF7BD00A. However subtle the alteration—an omitted period or extra space—the hash value changes markedly. The chance of an altered electronic document having the same MD5 hash—a "collision," in cryptographic parlance—is 1 in 340 trillion trillion trillion. Though supercomputers have fabricated collisions, this change still represents a level of reliability far exceeding that of fingerprint and DNA evidence.

Hashing sounds like rocket science—and it's a miraculous achievement—but it's very much a routine operation, and the programs used to generate digital fingerprints are freely available and easy to use. Hashing lies invisibly at the heart of everyone's computer and Internet activities⁶ and supports processes vitally important to electronic discovery, including identification, filtering, Bates numbering, authentication, and deduplication.

Knowing a file's hash value enables you to find its identical counterpart within a large volume of data without examining the contents of each file. The government uses this capability against nefarious Internet users, but in e-discovery it might be used to track down company secrets that disappeared when an employee joined the competition.

§ 4.4 Filtering and De-NISTing

A common e-discovery process is culling data collected from computers that couldn't be evidence because it isn't a custodian's work product. This process is done by matching hash values of collected data files to hash values on the National Software Reference Library's (NSRL) freely published list of hash values corresponding to common retail software and operating systems. The NSRL is part of the National Institute for Standards and Technology (NIST), so this process is commonly called "de-NISTing" a data set. For more information on the NSRL, visit **www.nsrl.nist.gov**/.

^{6.} For example, many web services store the hash value of your password, but not the password itself. This enables them to authenticate a user by comparing the hash of the password entered to the hash value on file; however, the password cannot be reverse engineered from the hash value. A remarkable feature of hash values is that they are one-way calculations, meaning that although the hash value identifies just one sequence of data, it reveals nothing about the data, much as a fingerprint uniquely identifies an individual but reveals nothing about their appearance or personality—it's computationally infeasible to derive the source data from the hash of the source data.

§ 4.5 Bates Numbering

Hashing's ability to uniquely identify e-documents makes it a candidate to supplement, though not supplant, traditional Bates numbering⁷ in electronic production. Though hash values don't fulfill the sequencing function of Bates numbers, they're excellent unique identifiers and enjoy an advantage over Bates numbers because they eliminate the possibility that the same number might be applied to different documents. An electronic document's hash value is derived from its contents, so it will never conflict with that of another document unless the two documents are identical. Similarly, because two identical documents from different custodians will hash identically, the documents' hash values won't serve to distinguish between the two despite their different origins.

Forensic examiners regularly use hashing to establish that a forensically sound duplicate of a hard drive faithfully reflects every byte of the source and to prove that their activities haven't altered the original evidence. As e-discovery gravitates to native production, concern about intentional or inadvertent alteration requires lawyers to have a fast, reliable method to authenticate electronic documents. Hashing neatly fills this bill. In practice, a producing party calculates and records the hash values of all items produced in native format. The slightest alteration of the data would be immediately apparent when the altered file is hashed.

The most important things for an attorney to know about hashing:

- 1. Electronically stored information of any type or size can be hashed
- 2. The algorithms used to hash data are not proprietary, and thus cost nothing to use
- 3. No matter the size of the file that's hashed, its hash value is *always* a fixed length
- 4. The two most common hash algorithms are called MD5 and SHA-1
- 5. In a random population of hashed data, no one can reverse engineer a file's hash value to reveal anything about the file

^{7.} Bates numbering has historically been employed as an organizational method to label and identify legal documents, especially those produced in discovery. "Bates" is capitalized because the name is derived from the Bates Manufacturing Company, which patented and sold auto-incrementing, consecutive-numbering stamping devices. Bates stamping served the dual functions of sequencing and uniquely identifying documents.

6. The chance of two different files accidentally having matching MD5 hash values is one in 340 trillion trillion—340 undecillion—so it is highly improbable that two files with matching hash values are not identical.

§ 4.6 Deduplication

In e-discovery, manually reviewing vast volumes of identical data is burdensome and poses a significant risk of conflicting relevance and privilege assessments. Hashing flags identical documents, permitting a single, consistent assessment of an item that might otherwise have cropped up hundreds of times and been mischaracterized many times. This is hash deduplication, and it drastically cuts review costs. But because even the slightest difference triggers different hash values, insignificant variations between files (e.g., different Internet paths taken by otherwise identical e-mail) may frustrate hash deduplication when hashing an entire electronic document. An alternative is to hash relevant segments of electronic documents to assess their relative identicality, a practice sometimes called "rear deduplication."

In practice, each file ingested and item extracted is hashed, and its hash value compared to the hash values of items previously ingested and extracted to determine if the file or item has been seen before. The first file is sometimes called the "pivot file," and any subsequent files with matching hashes are suppressed as duplicates. Instances of each duplicate and certain metadata is typically noted in a deduplication or "occurrence" log.

§ 4.7 Computers

Historically, all sorts of devices—and even people—were "computers." During World War II, human computers—women for the most part—were instrumental in calculating artillery trajectories and assisting with the challenging number-crunching needed by the Manhattan Project. Today, laptop and desktop personal computers spring to mind when we hear the term "computer," yet smart phones, tablet devices, global positioning systems, video gaming platforms, televisions, and a host of other intelligent tools and toys are also computers. More precisely, the central processing unit (CPU) or microprocessor of the system is the "computer," and the various input and output devices that permit humans to interact with the processor are termed "peripherals." The key distinctions between a mere calculator and a computer are the latter's ability to be programmed and its use cf memory and storage. The physical electronic and mechanical components of a computer are its hardware, and the instruction sets used to program a computer are its software. Unlike the interchangeable cams of Pierre Jaquet-Droz's mechanical doll, modern electronic computers receive their instructions in the form of digital data typically retrieved from the same electronic storage medium as the digital information upon which the computer performs its computational wizardry.

When you push the power button on your computer, you trigger an extraordinary, expedited education that takes the machine from insensible illiterate to worldly savant in a matter of seconds. The process starts with a snippet of data on a chip called the "ROM BIOS" storing just enough information in its "read only memory" to grope around for the "basic input and output system" peripherals (like the keyboard, screen, and most importantly, the hard drive). The ROM BIOS also holds the instructions needed to permit the processor to access more and more data from the hard drive in a widening gyre, "teaching" itself to be a modern, capable computer.

This rapid, self-sustaining self-education is as magical as if you lifted yourself into the air by pulling on the straps of your boots, which is truly why it's called "bootstrapping," or just "booting," a computer.



Figure 4-10: Computer interior

Computer hardware shares certain common characteristics. Within the CPU, a microprocessor chip is the computational "brains" of the system and resides in a socket on the motherboard, a rigid surface etched with metallic patterns serving as the wiring between the components on the board. The microprocessor generates considerable heat, necessitating the attachment of a heat dissipation device called a heat sink, often abetted by a fan. The motherboard also serves as the attachment point for memory boards (grouped as modules, or "sticks") called "RAM" for "random access memory." RAM serves as the working memory of the processor while it performs calculations; accordingly, the more memory present, the more information can be processed at once, enhancing overall system performance. See Figure 4-10.

Other chips comprise a graphics processor unit (GPU) residing on the motherboard or on a separate expansion board called a video card or graphics adapter. The GPU supports the display of information from the processor onto a monitor or projector and has its own complement of memory dedicated to superior graphics performance. Likewise, specialized chips on the motherboard or an expansion board called a "sound card" support the reproduction of audio to speakers or a headphone. Video and sound processing capabilities may even be fully integrated into the microprocessor chip.

The processor communicates with networks through an interface device called a "network adapter," which connects to the network physically through a LAN port or wirelessly using a Wi-Fi connection.

Users convey information and instructions to computers using tactile devices like a keyboard, mouse, or track pad, but may also employ voice or gestural recognition mechanisms.

Persistent storage of data is a task delegated to other peripherals: optical drives (CD-ROM and DVD-ROM devices), floppy disk drives, solid-state media (i.e., thumb drives), and most commonly, hard drives.

All the components just described require electricity, supplied by batteries in portable devices or by a power supply converting AC current to the lower DC voltages required by electronics.

From the standpoint of electronic discovery, it's less important to define these devices than it is to fathom the information they hold, the places it resides, and the forms it takes. Parties and lawyers have been punished for their failure to inquire into and understand the roles computers, hard drives, and servers play as repositories of electronic evidence. Moreover, much money spent on electronic discovery today is wasted because of parties' efforts to convert ESI to paper-like forms instead of learning to work with ESI in the forms in which it customarily resides on computers, hard drives, and servers.

§ 4.7:1 Sectors and Clusters and Tracks, Oh My!

Recall the discussion of electromagnetic hard drives earlier in the chapter. When manufactured, a hard drive's platters are organized into specific structures to enable the organized storage and retrieval of data. This is low-level formatting, dividing each platter into tens of thousands of densely packed concentric circles called "tracks." If you could see them (and you can't because they are nothing more than microscopic magnetic traces), they might resemble the growth rings of the world's oldest tree. It's tempting to compare platter tracks to a phonograph record, but a phonograph record's track is a single spiraling groove, not concentric circles. A track holds far too much information to serve as the smallest unit of storage on a disk, so each one is further broken down into physical sectors. A sector is normally the smallest individually addressable unit of information stored on a hard disk, and it held 512 bytes of information until about 2010. Today, sector sizes vary, but tend to be 4,096 bytes. Figure 4-11 shows a very simplified representation of a platter divided into tracks and sectors; the number of tracks and sectors is far, far greater that the illustration suggests. Additionally, the layout of sectors isn't symmetrical, but zoned to allow the inclusion of more sectors per track as the tracks enlarge away from the spindle.



Figure 4-11: Hard drive platter

Introduction to Digital Data, Computers, and Storage Media

To this point, we have described only physical units of storage. That is, platters, tracks, sectors, and even bits and bytes exist as discrete physical manifestations written to the media. Computers manage data not only physically, but also logically. As it's impractical to manage and gather the data by assembling it from sectors, operating system speed up the process by grouping sectors into contiguous chunks of data called "clusters."

A cluster is the smallest amount of disk space that can be allocated to hold a file. Computers organize hard disks based on clusters, which consist of one or more contiguous sectors. The smaller the cluster size, the more efficiently a disk stores information. Conversely, the fewer the number of clusters, the less space is consumed by the table required to track their content and locations.

To recap, data is stored in logical units called clusters, made up of multiple physical storage units termed sectors. A series of logical clusters, in turn, comprise tracks (concentric circles or "tree rings" of data) on platters, one or more disks of rotating electromagnetic storage media within the enclosure of a mechanical hard drive. When tracks overlie one another on both sides of a platter and across multiple platters, this is termed a cylinder (although "cylinder" is an archaic term from the days when hard drive storage was tied to the physical geometry of the formatted disks). So, the order of data capacity is: bits > bytes > sectors > clusters > tracks > cylinders > platters > drive.

§ 4.7:2 Operating Systems and File Systems

As hard disks have grown exponentially in size, using them efficiently is increasingly difficult. A library with thirty books runs much differently than one with thirty billion. "File system" is the name given to the logical structures and software routines used to control access to the storage on a hard disk system and the overall structure in which files are named, stored, and organized. An "operating system" is a large and complex collection of functions, including the user interface and control of peripherals like printers. Operating systems are built on file systems. If the operating system is the car, then the file system is its chassis. Operating systems are known by familiar household names like MS-DOS, Windows, or MacOS. In contrast, file systems go by obscure monikers like FAT, FAT32, ext2, NFTS, and HFS+.

§ 4.7:3 NTFS File Systems

The NTFS file system at the heart of Microsoft Windows environments like Windows NT, 2000, XP, Vista, and Windows 7 through 10 accounts for most personal computers in the world; however, there are many non-Microsoft operating systems out there, such as Unix, Linux, and MacOS. Though similarities abound, these other operating systems use different file systems, and the Unix or Linux operating systems often lie at the heart of corporate and web file servers—today's "big iron" systems and cloud computing. As well, MacOS usage has grown markedly as Apple products have kicked down the door of business computing and have captivated consumers.

NTFS uses a powerful and complex file system database called the Master File Table, or MFT, to manage file storage. Understanding the file system is key to appreciating why deleted data doesn't necessarily go away. It's the file system that marks a file as deleted even though it leaves the data on the drive. It's the file system that enables the creation of multiple partitions where data can be hidden from prying eyes. Finally, it's the file system that determines the size of a disk cluster with the attendant persistence of data within the slack space. Exactly what all this means will be clear shortly.

§ 4.7:4 Formatting and Partioning

Partitioning divides drives into volumes that users see as drive letters (e.g., C:, E:, F:, and so on). Formatting defines the logical structures on the partition and places necessary operating system files at the start of the disk to facilitate booting. For most users, their computer comes with the hard drive partitioned as a single volume (universally called "C:"). Some users will find (or will cause) their hard drive to be partitioned into multiple volumes, each appearing to the user as if it were an independent disk drive. Partitions can be designated "active" and "inactive." Only one partition may be designated as active at any given time, and that partition is the one that boots the computer. The significance in discovery is that inactive partitions are invisible to anyone using the computer unless they know to look for them and how to find them. Inactive partitions are a place where users with something to conceal from prying eyes may choose to hide it.

§ 4.7:5 Data Recovery and File Carving

A computer manages its hard drive in much the same way a librarian manages a library. The files are the "books" and their location is tracked by an index. But there are two key differentiators between libraries and computer file systems. Computers

employ no Dewey Decimal System, so electronic "books" can be on any shelf. Further, electronic "books" may be split into chapters and those chapters stored in multiple locations across the drive. This is called "fragmentation." Historically, libraries tracked books by noting their locations on index card in a card catalog. Computers similarly employ directories (called "file tables") to track files and fragmented segments of files.

When a user hits "Delete" in a Windows environment, nothing happens to the actual file targeted for deletion. Instead, a change is made to the master file table that keeps track of the file's location. Thus, akin to tearing up a card in the card catalog, the file, like its literary counterpart, is still on the "shelf." But now—without a locator in the file table—the deleted file is a needle in a haystack, buried amidst millions of other unallocated clusters. To recover the deleted file, a computer forensic examiner employs three principal techniques detailed below.

File Carving by Binary Signature: Because most files begin with a unique digital signature identifying the file type, examiners run software that scans each of the millions of unallocated clusters for file signatures, hoping to find matches. If a matching file signature is found and the original size of the deleted file can be ascertained, the software copies, or "carves out," the deleted file. If the size of the deleted file is unknown, the examiner designates how much data to carve out. The carved data is then assigned a new name and the process continues.

Unfortunately, deleted files may be stored in pieces, as discussed above, so simply carving out contiguous blocks of fragmented data grabs intervening data that has no connection to the deleted file and fails to collect segments for which the directory pointers have been lost. Likewise, when the size of the deleted file isn't known, the size designated for carving may prove too small or large, leaving portions of the original file behind or grabbing unrelated data. Incomplete files and those commingled with unrelated data are generally corrupt and nonfunctional. Their evidentiary value is also compromised.

File signature carving is frustrated when the first few bytes of a deleted file are overwritten by new data. Much of the deleted file may survive, but the data indicating what type of file it was, thus enabling its recovery, is gone.

File signature carving requires that each of the file types sought to be recovered is searched for in each unallocated cluster. When a court directs that an examiner "recover all deleted files," it's an exercise that could take excessive effort followed by countless hours spent examining corrupted files. Instead the protocol should, as feasi-

ble, specify the particular file types of interest based on how the machine was used and the facts and issues in the case.

Notably, file carving of deleted information from unallocated clusters is fast becoming untenable by the emergence of solid-state and encrypted media. Storage optimization techniques used by solid-state drives serve to routinely overwrite once recoverable data.

File Carving by Remnant Directory Data: In some file systems, residual file directory information revealing the location of deleted files may be strewn across the drive. Forensic software will scan the unallocated clusters in search of these lost directories and use this data to restore deleted files. Here again, reuse of clusters can corrupt the recovered data.

Search by Keyword: Where it's known that a deleted file contained certain words or phrases, remnant data may be found using a keyword search of unallocated clusters. A keyword search is a laborious and notoriously inaccurate way to find deleted files, but it may find something when other techniques fail. If the keywords are too short or insufficiently precise, false positives follow ("noise hits"), obliging examiners to painstakingly examine each hit to assess relevance, then manually carve out responsive data.

§ 4.8 Servers

Servers were earlier defined as computers dedicated to a specialized task or tasks. But that definition doesn't begin to encompass the profound impact on society of the socalled "client-server" computing model. The ability to connect local "client" applications to servers via a network, particularly to database servers, is central to the operation of most businesses and to all telecommunications and social networking. Google and Facebook are merely enormous groupings of servers, and the Internet a vast, global array of shared servers.

§ 4.8:1 Local, Cloud, and Peer-to-Peer Servers

For e-discovery, let's divide the world of servers into three realms: local, cloud, and peer-to-peer server environments.

Local servers employ hardware that's physically available to the party that owns or leases the servers. Local servers reside in a computer room on a business's premises or in leased equipment "lockers" accessed at a colocated data center where a lessor furnishes, for example, premises security, power, and cooling. Local servers are easiest to deal with in e-discovery because physical access to the hardware supports more and faster options when it comes to preservation and collection of potentially responsive ESI.

Cloud servers typically reside in facilities not physically accessible to persons using the servers, and servers are not typically dedicated to a single user. Instead, the cloud computing consumer is buying services via the Internet that emulate the operation of a single machine or a room full of machines, all according to the changing needs of the cloud consumer. Webmail is the most familiar form of cloud computing, in a variant called "SaaS" (for software as a service). Webmail providers like Google, Yahoo, and Microsoft make e-mail accounts available on their servers in massive data centers, and the data on those servers is available solely via the Internet with no user having the right to gain physical access to the machines storing their messaging.

Peer-to-peer (P2P) networks exploit the fact that any computer connected to a network has the potential to serve data across the network. Accordingly, P2P networks are decentralized; that is, each computer, or "node," on a P2P network acts as client and server, sharing storage space, communication bandwidth, and/or processor time with other nodes. P2P networking may be employed to share a printer in the home, where the computer physically connected to the printer acts as a print server for other machines on the network. On a global scale, P2P networking is the technology behind file-sharing applications like BitTorrent that have garnered headlines for their facilitation of illegal sharing of copyrighted content. When users install P2P applications to gain access to shared files, they simultaneously (and often unwittingly) dedicate their machine to serving up such content to a multitude of other nodes.

§ 4.8:2 Virtual Servers

Though we've so far spoken of server hardware (i.e., physical devices), servers may also be implemented virtually, through software that emulates the functions of a physical device. Such "hardware virtualization" allows for more efficient deployment of computing resources by enabling a single physical server to host multiple virtual servers.

Virtualization is the key enabling technology behind many cloud services. If a company needs powerful servers to launch a new social networking site, it can raise capital and invest in the hardware, software, physical plant, and personnel needed to support a data center, with the attendant risk that it will be over-provisioned or underprovisioned as demand fluctuates. Alternatively, the start-up can secure the computing resources it needs by using virtual servers hosted by a cloud service provider like Amazon or Microsoft. Virtualization permits computing resources to be added or retired commensurate with demand, and being pay-as-you-go, it requires little capital investment. Thus, a computing platform or infrastructure can be virtualized and leased; in other words, offered as a service via the internet. Accordingly, cloud computing is sometimes referred to as PaaS (platform as a service) and IaaS (infrastructure as a service). Web-based applications are SaaS (software as a service).

It's helpful for attorneys to understand the role of virtual machines (VMs) because the ease and speed with which VMs are deployed and retired, as well as their isolation within the operating system, can pose unique risks and challenges in e-discovery, especially with respect to implementing a proper legal hold and when identifying and collecting potentially responsive ESI.

§ 4.8:3 Server Applications

Computers dedicated to server roles typically run operating systems optimized for server tasks and applications specially designed to run in a server environment. In turn, servers often support dedicated tasks, such as serving webpages (web server), retaining and delivering files from shared storage allocations (file server), organizing voluminous data (database server), facilitating the use of shared printers (print server), running programs (application server), or handling messages (mail server). These various server applications may run physically, virtually, or as a mix of the two.

§ 4.9 Network Shares

Sooner or later, all electronic storage devices fail. Even the RAID storage arrays previously discussed do not forestall failure, but instead afford a measure of redundancy to allow for replacement of failed drives before data loss. Redundancy is the sole means by which data can be reliably protected against loss; consequently, companies routinely back up data stored on server NAS and SAN storage devices to backup media like magnetic tape or online (e.g., cloud) storage services. However, individual users often fail to back up data stored on local drives. Accordingly, enterprises allocate a "share" of network-accessible storage to individual users and "map" the allocation to the user's machine, allowing use of the share as if it were a local hard drive. When the user stores data to the mapped drive, that data is backed up along with the contents of the file server. Although network shares are not local to the user's computer, they are typically addressed using drive letters (e.g., M: or T:) as if they were local hard drives.

§ 4.10 Practice Tips for Computers, Hard Drives, and Servers

Your first hurdles when dealing with computers, hard drives, and servers in e-discovery are to identify potentially responsive sources of ESI and take appropriate steps to inventory their relevant contents, then note the form and associated metadata of the potentially responsive ESI and preserve it against spoliation. Get a handle on data volumes, file types, metadata, replicatior, and distribution as early in the litigation process as possible since these determine the overall cost to preserve, collect, process, and host ESI in discovery.

Take stock of physical computing and storage devices. For each machine or device holding potentially responsive ESI, you may wish to collect the following information:

- Manufacturer and model
- Serial number and/or service or asset tag
- Operating system
- Custodian
- Location
- Type of storage (don't miss removable media like SD and SIM cards)
- Aggregate storage capacity (in MB, GB, or TB)
- Encryption status
- Credentials (user IDs and passwords), if encrypted
- Prospects for upgrade or disposal

If you'll preserve ESI by drive imaging, it's helpful to identify device interfaces.

For servers, further information might include the following:

- Purpose(s) of the server (e.g., web server, file server, print server)
- Names and contact information of server administrator(s)
- Time in service and data migration history

- Whether hardware virtualization is used
- RAID implementation(s)
- Users and privileges
- Logging and log retention practices
- Backup procedures and backup media rotation and retention
- Whether the server is "mission critical" and cannot be taken offline or can be downed

When preserving the contents of a desktop or laptop computer, it's typically unnecessary to sequester any component of the machine other than its hard drive(s) since the ROM BIOS holds little information beyond the rare forensic artifact. Before returning a chassis to service with a new hard drive, be sure to document the custodian, manufacturer, model, and serial number/service tag of the redeployed chassis, retaining this information with the sequestered hard drive.

The ability to fully explore the contents of servers for potentially responsive information hinges on the privileges extended to the user. Be sure that the person tasked to identify data for preservation or collection holds administrator-level privileges.

Above all, remember that computers, hard drives, and servers are constantly changing while in service. Simply rebooting a machine alters system metadata values for large numbers of files. Accordingly, you should consider the need for evidentiary integrity before exploring the contents of a device, at least until appropriate steps are taken to guard against unwitting alteration. Note also that connecting an evidence drive to a new machine effects changes to the evidence unless suitable write-blocking tools or techniques are employed.

§ 4.11 Conclusion: Takeaways on Electronically Stored Information

- 1. Common law imposes a duty to preserve potentially relevant information in anticipation of litigation.
- 2. Most information is electronically stored information (ESI).
- 3. Understanding ESI entails knowledge of information storage media, encodings, and formats.
- 4. There are many types of e-storage media of differing capacities, form factors, and formats, like—

- (a) analog (phonograph record) or digital (hard drive, thumb drive, optical media), and
- (b) mechanical (electromagnetic hard drive, tape, etc.) or solid-state (thumb drive, SIM card, etc.).
- 5. Computers don't store text, documents, pictures, or sounds, they only store bits (1s or 0s).
- 6. Digital information is encoded as numbers by applying various encoding schemes, including—
 - (a) ASCII or Unicode for alphanumeric characters, and
 - (b) JPG for photos, DOCX for Word files, MP3 for sound files, etc.
- 7. We express these numbers in a base or radix (base 2 binary, 10 decimal, 16 hexadecimal, 60 sexagesimal). E-mail messages encode attachments in base 64.
- 8. The bigger the base, the smaller the space required to notate and convey the information.
- 9. Digitally encoded information is stored (written)-
 - (a) physically as bytes (8-bit blocks) in sectors and partitions, and
 - (b) logically as clusters, files, folders, and volumes.
- 10. Files use binary header signatures to identify file formats (type and structure) of data.
- 11. Operating systems use file systems to group information as files and manage filenames and metadata.
- 12. File systems employ filename extensions (e.g., .txt, .jpg, .exe) to flag formats.
- 13. All ESI includes a component of metadata (data about data) even if no more than what's needed to locate it.
- 14. A file's metadata may be greater in volume or utility than the contents of the file it describes.
- 15. File tables hold system metadata about the file (e.g., name, locations on disk, MAC dates)—it's context.
- 16. Files hold application metadata (e.g., EXIF geolocation data in photos, comments in docs)—it's content.

- 17. File systems allocate clusters for file storage; deleting files releases cluster allocations for reuse.
- 18. If unallocated clusters aren't reused, deleted files may be recovered ("carved") via computer forensics.
- 19. Forensic ("bitstream") imaging is a method to preserve both allocated and unallocated clusters.
- 20. Because data is numbers, data can be digitally "fingerprinted" using oneway hash algorithms (e.g., MD5, SHA-1).
- 21. Hashing facilitates identification, deduplication, and de-NISTing of ESI in e-discovery.
Chapter 5

E-Mail 101

Heather McFarlane

§ 5.1 Introduction

In lawsuits today, e-mail messages and their attachments provide the vast majority of discoverable information. By understanding the history and purpose of e-mail, as well as some of the technical attributes of e-mail, this chapter should assist in answering the following questions:

- How can I be sure that my client has properly searched for, preserved, and produced requested e-mail messages?
- How can I request e-mail in a way to get what I really want?
- What do I do if my opponent does not produce e-mail?
- How can I best mine e-mail messages and their attachments for information to further my case?
- How can I determine if an e-mail message is really what it purports to be so that I can introduce it into evidence or rely upon it for my case?

E-mail, of course, is only one component of electronic communication. This chapter does not discuss text messages, chat communication, or exchanges made on collaborative work sites,¹ although data created in these forms is likely to continue to grow in size and importance.

^{1.} A "collaborative work site" is a term given to computer programs that allow multiple people to share information and work together simultaneously. This could include sharing calendar information with available conference rooms. It could also refer to programs, such as Google Docs, that allow multiple authors to work on the same document together. Some of these programs allow the tracking of each author's input, which could leave a trail of electronic information. In a case regarding an ambiguous contract, for example, it might be helpful to know which author made which change or suggestion.

§ 5.2 Ethics Requires Lawyers to Understand E-Mail

In August 2012, the American Bar Association amended rule 1.1, "Competence," to include a comment explaining that lawyers have a duty to understand changing technology and how it affects their clients in litigation:

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.²

This comment reflects a growing concern that lawyers do not adequately understand electronic discovery ("e-discovery") and how it impacts their clients.

As case law has made clear, it is not enough for a lawyer to plead ignorance when faced with e-discovery questions. On the other hand, lawyers need not be perfect either; only a good faith effort must be made. What is a good faith effort?

First, lawyers must understand their clients' information technology systems, the key players in the litigation, and take an active role in preserving documents that may relate to the litigation.³ Further, the lawyer must continue to remain involved to oversee the e-discovery process.⁴ Understanding e-mail and how it works technically can be the first step in discharging the duty.

§ 5.3 History of E-Mail

The concept of electronically messaging for communication first arose in 1971 when Ray Tomlinson first sent some text from one computer in his office to another.⁵ This first message transfer is most analogous to instant messaging as we know it today. Tomlinson was the person who decided to use the @ symbol that the world has come to use for addressing e-mail.⁶ The information before the @ symbol denotes the specific addressee, much like the name written on the first line of an envelope. The infor-

^{2.} Model Rules of Prof'l Conduct R. 1.1 cmt. 8 (2012).

^{3.} Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432–33 (S.D.N.Y. 2004).

^{4.} Zubulake, 229 F.R.D. at 432-33.

^{5.} All Things Considered: The Man Who Made You Put Away Your Pen, National Public Radio (Nov. 21, 2009).

^{6.} NPR, The Man Who Made You Put Away Your Pen.

mation after the @ symbol indicates the location where the information should be

sent; this is much like the next two lines of an address on an envelope. Interestingly, Tomlinson chose this symbol because it was physically present on the standard keyboard and it was the only preposition available on the keyboard.⁷

E-mail as we know it today was born several years later in 1978. A group of doctors at the University of Medicine and Dentistry in Newark, New Jersey, hired fourteen-yearold V. A. Shiva Ayyadurai to convert their traditional interoffice mail system into an electronic one.⁸ Ayyadurai attempted to literally replicate the process of physical mail into an electronic format.⁹ To do this, Ayyadurai observed how the doctors at the hospital created, sent, and received physical mail.¹⁰ He watched as secretaries typed memoranda, attached actual carbon copies of relevant attachments, and placed the communication in a container that was then sent through a physical tube like the ones used in some bank drive-through services today.¹¹ He knew that he needed to create a system—one that included inboxes, outboxes, and file folders—for users to adopt this new method of communication.¹²

Today, the public has accepted electronic mail, and the volume of e-mail continues to grow. This means e-mail is here to stay in our society, and it is here to stay for discovery in lawsuits.

§ 5.4 Volume of E-Mail Compared to Physical Mail

By way of illustration, the following chart shows the volume of the U.S. Postal Service mail in relation to the estimate of worldwide e-mail. As a caveat, I may agree with a phrase popularized by Mark Twain: "There are three kinds of lies: lies, damned lies, and statistics." In researching the volume of mail versus e-mail, it was easy to determine the actual volume of physical mail in the United States, because the U.S. Postal Service submits an annual report to Congress each year that includes the number of pieces of mail it handled. The volume of worldwide e-mail, however, varies by orders of magnitude, depending on the source. Nonetheless, everyone seems to agree

§ 5.4

^{7.} NPR, The Man Who Made You Put Away Your Pen.

^{8.} Doug Aamoth, *The Man Who Invented Email*, Time Tech (2011), http://techland.time.com/ 2011/11/15/the-man-who-invented-email, at 1.

^{9.} Aamoth, The Man Who Invented Emcil, at 2.

^{10.} Aamoth, The Man Who Invented Emcil, at 2.

^{11.} Aamoth, The Man Who Invented Emcil, at 2.

^{12.} Aamoth, The Man Who Invented Emcil, at 2.

that worldwide e-mail vastly outpaces physical mail. The following numbers, for the most part, come from research completed by V. A. Shiva Ayyadurai.¹³

Year	Physical mail articles	E-mail
1979	100 billion	10,000
1981	110 billion	750,000
1983	119 billion	500 million
1985	140 billion	1.5 billion
1988	161 billion	3 billion
1989	162 billion	5 billion
1991	166 billion	15 billion
1993	171 billion	50 billion
1995	181 billion	100 billion
1997	191 billion	550 billion
1999	202 billion	4 trillion
2003	202 billion	40 trillion
2005	212 billion	50 trillion
2007	212 billion	70 trillion
2008	203 billion	85 trillion
2009	177 billion	100 trillion
2010	171 billion	120 trillion
2011	168 billion	150 trillion
2012	160 billion	180 trillion
2015	154.3 billion	n/a

^{13.} The estimate of U.S. Postal Service mail volume from 1978 to 1980 comes from research compiled by V.A. Shiva Ayyadurai and displayed in a helpful graphic timeline at www.vashiva.com/ innovation/email/vashiva-the-history-of-email-vs-usps-snail-mail.asp. The volume of U.S. Postal Service mail from 2008 to 2012 comes from the U.S. Postal Service's annual report to Congress and can be found at http://about.usps.com/publications/annual-report-comprehensive-statement-2012/ annual-report-comprehensive-statement-2012.pdf. The latest U.S. Postal Service data (2015–2018) is found at https://facts.usps.com/table-facts/.

Year	Physical mail articles	E-mail
2016	154.3 billion	n/a
2017	149.5 billion	n/a
2018	146.4 billion	n/a
2020 (projected)	130 billion	500 trillion

To put the e-mail volume in perspective, the Radicati Group reports that there were more than 3.8 billion e-mail users during 2018, which means that over half the planet currently uses e-mail. Radicati estimates that users sent and received about 281 billion e-mails per day in 2018. That number is expected to reach 4.2 billion users sending 333 billion e-mails per day by the end of 2022.¹⁴

Each e-mail user has an average of 1.75 email accounts. Google alone had over 1 billion active email users in 2016.¹⁵

^{14.} Heinz Tschabitscher, How Many People Use Email Worldwide?, Lifewire (June 24, 2019), www.lifewire.com/how-many-email-users-are-there-1171213.

^{15.} Tschabitscher, How Many People Use Email Worldwide?



Number of active Gmail users worldwide from January 2012 to October 2019 (in millions)¹⁶

© Statista 2019 🗯

To further complicate matters, many users open the same e-mail on a mobile device and on a computer. To use myself as an example, I have three active e-mail accounts, and I have directed all three of them to arrive on my iPhone, my iPad, and my iMac. As will be discussed later, this practice of opening accounts from different devices can seriously impact efforts to collect and maintain e-mail in discovery, depending on the user's e-mail provider.

E-mail pervades communication in the corporate world, and it continues to grow in importance. In 2017, Forbes reported that "office workers receive at least 200 [e-mail] messages a day and spend about two-and-a-half hours reading and replying to emails."¹⁷

^{16.} J. Clement, chart "Number of Active Gmail Users Worldwide from January 2012 to October 2018 (in millions)," Statista (Jan. 18, 2019), www.statista.com/statistics/432390/active-gmail-users/.

^{17.} Annabel Acton, *How To Stop Wasting 2.5 Hours On Email Every Day*, Forbes (July 13, 2017), www.forbes.com/sites/annabelacton/2017/07/13/innovators-challenge-how-to-stop-wasting-time-on-emails/.

The volume of e-mail and its pervasive use tells only part of the story of how e-mail impacts discovery. In the world of paper files, people were more careful in deciding what to keep and maintain. Paper files take up valuable physical space, which encourages people to limit what they save. Paper files also require more administrative time in creating folders, copying the paper, and filing it in the appropriate place. E-mail, cn the other hand, allows each user to arbitrarily determine what to keep, how to keep it, and where to put it. The only limitation on e-mail is the size of the e-mail storage account—and that is assuming that users don't export the data elsewhere (for example, forwarding e-mail messages from one account to another, or downloading it to another media source). Further, unlike physical file cabinets, e-mail is stored in massive data sets that require software to read and organize it.

§ 5.5 What Is E-Mail?

E-mail, as discussed in this chapter, refers to the electronic system of communication that most closely resembles physical correspondence. The word system should be the focus, because not all e-mail is transmitted in the same way. These differences in transmission can be important when determining how to preserve, locate, and produce e-mail.

By way of analogy, think of the U.S. Postal Service. The U.S. Postal Service has multiple, complex sub-systems that process, store, and transport tangible communication and things. The systems and locations of various cities can vary, but these variations can only work together if people who use the U.S. Postal Service follow certain rules to ensure proper delivery.¹⁸ These rules, which are called protocols in the e-mail world, dictate the size of the envelope, the placement of the address and return address, the amount of postage, and the use of a zip code. These parameters allow the system of electronically scanning and applying a barcode to ensure proper delivery.¹⁹

Similarly, a number of e-mail providers provide sub-systems for e-mail creation, storage, and transmission. At its core, an e-mail message is a plain text file. Any non-text attachment—such as a picture, Microsoft Word document, or other application-based data file—may only be transmitted through e-mail by encoding or changing that nontext information into a text file. When the e-mail message reaches the recipient, the recipient's e-mail provider translates this code to allow access to the attachment. The

^{18.} Lee Ann Obringer, *How the U.S. Postal Service Works*, HowStuffWorks, http://people. howstuffworks.com/usps.htm.

^{19.} Obringer, How the U.S. Postal Service Works.

programming in the recipient's e-mail system determines the way the resulting e-mail appears.

The remaining, or hidden, information, such as the locations of the systems sending and receiving the e-mail message, can also be seen, captured, and used in litigation. These fields, known as metadata, are not always easy to see. For an illustration, the see the following header of an e-mail from my paralegal:

Received: from ORD2MBX01H.mex05.mlsrvr.com ([fe80: <u>11f4:d169:375f:62d2</u>]) by ORD2HUB26.mex05.mlsrvr.com ([fe80::be30:5bff:fef4:9240%15]) with <u>mapp</u> i id 14.03.0158.001; Wed, 23 Oct 2013 13:27:43 -0500
Content-Type: application/mstnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Lynda Hart < hart@thekubiaklawfirm.com>
To: Heather Kubiak <hkubiak@icloud.com>, Heather Kubiak</hkubiak@icloud.com>
<hkubiak@thekubiaklawfirm.com></hkubiak@thekubiaklawfirm.com>
Subject: RE: Status of E-Discovery Article
Thread-Topic: Status of E-Discovery Article
Thread-Index: AQHO0B110Zb2Zt7MyEyEjHb4yT8uqJoCmrjQ
Date: Wed, 23 Oct 2013 13:27:42 -0500
Message-ID: <c8f0625f241f1e47a45052752b3410a27a0c176e@ord2mbx01h.mex05.mlsrvr.com></c8f0625f241f1e47a45052752b3410a27a0c176e@ord2mbx01h.mex05.mlsrvr.com>
References: <8cf8b33a-6044-4acd-b663-ad153ed0b31a@me.com>
In-Reply-To: <8cf8b33a-6044-4acd-b663-ad153ed0b31a@me.com>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <c8f0625f241f1e47a45052752b3410a27a0c176e@ord2mbx01h.mex05.mlsrvr.com></c8f0625f241f1e47a45052752b3410a27a0c176e@ord2mbx01h.mex05.mlsrvr.com>
MIME-Version: 1.0
X-MS-Exchange-Organization-AuthSource: ORD2HUB26.mex05.mlsrvr.com
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [67.200.230.146]
X-MS-Exchange-Organization-AVStamp-Mailbox: SMEXtG1w;1035900;0;This mail has
been scanned by Trend Micro ScanMail for Microsoft Exchange;

All of the information contained in the header is in reverse chronological order and tracks the journey that the message took from the sender to the recipient. The first word found in the e-mail header is "Received," which indicates that the message has successfully been transmitted and delivered. The bottom of the header contains the "Originating-IP [Internet protocol]" address. Much like a letter goes through several post offices on its way from the sender to the recipient, an e-mail may go through multiple mail servers. Because of the reverse chronological order, the information at the top of the header is the last stop along that journey; that is, "received" (which would more accurately be described as "delivered").

The e-mail header also contains identification codes, which are assigned by the various servers it encounters. These codes are unique and allow system administrators to track the message in the server logs. The identification code for this e-mail is:

Message-ID: <C8F0625F241F1E47A45052752B3410A27A0C176E@ORD2MBX-01H.mex05.mlsrvr.com>

Near the bottom of the e-mail is the originating IP address, which more specifically identifies the location of the Internet connection (not the location of the sender) from which the message was transmitted:

X-Originating-IP: [67.200.230.146]

The IP address is potentially the most critical information contained in the header. It can be used to trace the message back to an Internet connection and often to the actual device that sent the message. Using this information can allow a user to identify the origination of the e-mail to assess potential fraud. The "from" section can be thought of as the return address on an envelope, whereas the IP address is more closely related to the postmark. An IP address is more difficult to fake, although not impossible.

The lines just above the originating IP show the path that the message took from the sender to the recipient. It passed through an MS-Exchange server identified as "ORD2HUB25.mex05.mlsrvr.com." The information also shows that the message was formatted in MIME Version 1.0 (computer language), was transmitted in English (US), and had no attachments.

Accept-Language: en-US Content-Language: en-US X-MS-Has-Attach: X-MS-Exchange-Organization-SCL: -1 X-MS-TNEF-Correlator: <C8F0625F241F1E47A45052752B3410A27A0C176E@ORD2MBX-01H.mex05.mlsrvr.com> MIME-Version: 1.0 X-MS-Exchange-Organization-AuthSource: ORD2HUB26.mex05.mlsrvr.com X-MS-Exchange-Organization-AuthAs: Internal X-MS-Exchange-Organization-AuthMechanism: 04

These lines indicate that Lynda is replying to an e-mail and references the e-mail identification, which was assigned to the original e-mail:

References: <8cf8b33a-6044-4acd-b663-ad153ed0b31a@me.com> In-Reply-To: <8cf8b33a-6044-4acd-b663-ad153ed0b31a@me.com>

Just below the notation showing that the e-mail has been received is information that identifies the content type and how (and if) the e-mail was encoded.

Content-Type: application/ms-tnef; name="winmail.dat" Content-Transfer-Encoding: binary

The following information contained in the e-mail header identifies the sender, recipient, subject, and date and time that the message was transmitted:

From: Lynda Hart <lhart@thekubiaklawfirm.com> To: Heather Kubiak <hkubiak@icloud.com>, Heather Kubiak <hkubiak@thekubiaklawfirm.com> Subject: RE: Status of E-Discovery Article Thread-Topic: Status of E-Discovery Article Thread-Index: AQHO0B110Zb2Zt7MyEyEjHb4yT8uqJoCmrjQ Date: Wed, 23 Oct 2013 13:27:42 -0500

The "from" field is the least reliable part of the e-mail header. Scammers can insert anything they want into the "from" field, including an address that they made up or the address of innocent third parties.

It is important to note that the timestamp for the message is given as the sender's local time (based upon the clock settings on the sending device) followed by "0500," which indicates the number of hours' difference between the sender's time and Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). This time offset information gives an indication to the location of the device that sent the message. If the offset

time does not accurately correspond with the purported sender's time zone, that is further indication of potential fraud.

§ 5.6 How Does E-Mail Work?

To help locate responsive e-mail messages in discovery (and in implementing legal holds), it is helpful to understand how e-mail works. To illustrate, I have created the following graphic:



How E-Mail Works

For e-mail to be properly delivered, each user has a unique e-mail address, which is composed of their personal identification (recipient name) followed by @ and the domain name.

When an e-mail is composed and the sender hits "send," the e-mail connects to the sender's Simple Mail Transfer Protocol (SMTP) server, which takes the "to" address and breaks it down into the two parts separated by the @ symbol. The SMTP server is similar to the local post office in that it confirms the e-mail is properly addressed and directs the e-mail to the next stop along its journey to the recipient. The SMTP server then communicates with the Domain Name System (DNS), which translates the recipient's e-mail domain to an IP address. Once the sender's SMTP server has this destination information, then the e-mail is able to be transferred to the recipient's SMTP server. The recipient's SMTP server routes the message to a Mail Transfer Agent (MTA) (similar to a local postal carrier in this post office analogy), which is then able to take the recipient name (portion before the @ symbol) and direct the incoming mail to the appropriate mailbox.

Now comes the tricky part: different e-mail services deliver and maintain e-mail messages differently. On the above chart that shows "My Server," the type of protocol that the e-mail system uses will determine where e-mail will reside. Here is a chart of the common types of e-mail systems, how they work, and examples of providers using these systems:

Protocol Type	How It Works
"POP3"—Post Office Protocol (Version 3)	Post Office Protocol 3 (POP3) servers hold incoming e-mail messages until you check your e-mail, at which point they're transferred to your computer. POP3 is the most common account type for personal e-mail. Messages are typically deleted from the server when you check your e-mail. Unless configured properly, an e-mail message will only appear on the first device that accesses the e-mail.

Protocol Type	How It Works
IMAP	Internet Message Access Protocol (IMAP) servers let you work with e-mail messages without downloading them to your computer first. You can preview, delete, and organize messages directly on the e-mail server, and copies are stored on the server until you choose to delete them. IMAP e-mail messages allow all of a user's devices to receive the same e- mail message. IMAP is commonly used for business e-mail accounts.
MAPI	Microsoft calls its proprietary e-mail protocol MAPI, or Messaging Application Programming Interface. Outlook uses MAPI in conjunction with a Microsoft Exchange Server mail server. MAPI requires a secure Internet connection. It also allows for "synching." Deleting or filing an e-mail message on one device will also do the same task on other devices.
НТТР	 Hypertext Transfer Protocol (HTTP) is used to display webpages, but it can also be used to send and receive e-mail. HTTP protocol allows a user to access e-mail from remote locations from the cloud (see section 5.7 below). Usually, a user has a limited amount of space on that server and must delete or move information before creating or receiving additional information.

As the above chart explains, the location of potentially responsive e-mail messages can depend upon the e-mail system used by the sender and recipient. It also illustrates the need to thoroughly understand the client and opposing party's technology.

§ 5.7 Trends and Products Impacting E-Discovery

It used to be the case that most corporate e-mail lived on that corporation's own server. The corporation controlled the server and determined how information would be handled and deleted. Because many corporations would also make backups of the data on its server, information sought in discovery may also be found on backup devices and locations. Today, most e-mail service providers supply "cloud" services. The "cloud" describes a place that holds information accessible to the subscriber, but not housed on a local computer.

G Suite (formerly Google Apps) is a common resource used to store information and process e-mails, especially for small and medium-sized businesses. In keeping with the need to freeze information and prevent automatic, unintentional, or even intentional manipulation of information, G Suite allows the user to place a litigation hold on stored information.²⁰ Google advertises that the litigation hold will preserve all e-mail messages and attachments in a user's mailbox at the time the hold is placed, including sent mail, drafts, trash, and spam. Google also states that e-mail can be searched by custodian, date, and time. Finally, G Suite allows the administrator to prevent users from deleting certain information from their accounts. "If a user who's subject to a hold deletes data, it's removed from the user's view, but the data is preserved in Vault. As long as the hold is in place, you can search and export that data."²¹

Microsoft Office 365 is another common e-mail provider. It contains e-discovery and analytics capabilities and offers a new solution called "Advanced eDiscovery," which provides an "end-to-end workflow to preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations. It also lets legal teams manage the entire legal hold notification workflow to communicate with custodians involved in a case."²²

In 2018, Gmail had 1.4 billion user accounts, and Office 365 had 120 million commercial users.²³ G Suite and Office 365 represent a shift from clients having complete control over their servers and information to Internet technology, something that may greatly impact e-discovery in the near future.

Google has recently introduced new security features, including automatic expiration and two-factor authentication. While these features are great from a security standpoint, they could create stumbling blocks with respect to e-discovery. Microsoft Out-

^{20.} The following site provides detailed instructions about placing a litigation hold in G Suite: https://support.google.com/vault/answer/2473591?hl=en.

^{21.} Place Gmail and classic Hangouts on hold, Google Vault Help, Google (2019), https://support.google.com/vault/answer/2473591?hl=en.

^{22.} Overview of the Advanced eDiscovery solution in Microsoft 365, Microsoft 365 compliance, Microsoft (July 9, 2019), https://docs.microsoft.com/en-us/office365/securitycompliance /compliance20/overview-ediscovery-20.

^{23.} The New Gmail: Emails (and Ediscovery) May Self-Destruct in 3...2...1, Zapproved (Apr. 30, 2018), www.zapproved.com/blog/ediscovery-ramifications-for-new-gmail-features/.

look has a similar e-mail expiration feature. "Data-gathering bots that are used to comb through electronic communications can't read data that isn't there."²⁴ "When e-mails expire, they disappear from the recipient's inbox or whatever folder it has been stored in on the recipient's end."²⁵ If an expiring e-mail is sent to a non-Gmail user, there will remain a trace, but "[t]he actual content will be gone, since it's stored (and deleted) elsewhere."²⁶

§ 5.8 Cooperation

If there is only one thing you take from this chapter, I hope it is my appeal to do whatever you can to cooperate on issues of e-discovery. Not only do the rules require it,²⁷ but the level of cooperation between opposing counsel and third parties directly impacts the cost of electronic discovery.

I highly recommend an in-person meet and confer, because dealing with a live body fosters cooperation more than talking on the telephone. Before meeting, it is helpful to send your opponent a list of questions you would like to discuss. Of course, be sure to answer these questions about your own client before you arrive at the meeting.

The twenty-five questions I find helpful are—

- What are the disputed issues in the case?
- Who are the witnesses or document custodians who might have knowledge of the case?
- Do the parties anticipate discovery of electronically stored information (ESI), including metadata?

25. Rachel Kraus, Google told us more cbout how that 'expiring emails' feature works, Mashable (Apr. 27, 2018), https://mashable.com/2018/04/27/new-gmail-expiring-emails-confidential-mode/.

^{24.} Tad Simons, *Will Gmail's New Security Features Complicate eDiscovery?*, Thomson Reuters (Aug. 13, 2018), www.legalexecutiveinstitute.com/gmail-security-ediscovery/.

^{26.} Kraus, Google told us more.

^{27.} Federal Rule of Civil Procedure 26(f) changed in 2006 to require parties to confer about e-discovery and to develop a plan. The parties must now report "any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced." Fed. R. Civ. P. 26(f)(3)(C). Although the Texas rule does not require a meet and confer, the Texas Supreme Court expects parties to meet and confer also. *See In re Weekley Homes, L.P.*, 295 S.W.3d 309, 315 n.6 (Tex. 2009). Claire Broadley provides a good summary of various states' position on e-discovery. *See E-Discovery: Learn How Data Turns Into Evidence in Legal Cases*, Who Is Hosting This? (Feb. 12 2019), www.whoishostingthis.com/resources/e-discovery/.

- Who is the pest person to explain the parties' information technology systems?
- When did the events involved in the lawsuit occur?
- What electronic programs did the parties use during the relevant time period?
- What types of information do the parties expect to exchange? Paper? Emails? Databases? Spreadsheets? Voicemail? Instant messaging? Security tapes or other video?
- Are personal e-mail accounts in play?
- What are the parties' data retention policies and practices, and how are those policies and practices implemented?
- What is the anticipated volume of paper and ESI?
- Will paper documents be scanned? If so, at what resolution, and will they be Bates labeled or processed for OCR (optical character recognition)? Who will pay for the scanning?
- What steps have been taken to preserve ESI?
- Do third parties have discoverable information about the case? If so, who should contact that party to ensure preservation of evidence?
- When did preservation duties arise, and how far into the future will they exist?
- When did various privileges come into play, and who are the potential people creating privileged material?
- Do the parties need a protective order?
- How will the parties handle inadvertent disclosure of privileged material?
- If the volume is large, how will the parties identify responsive and privileged material?
- Can the parties agree to keyword searches? If so, how will those words be identified? Will there be an opportunity after the initial searching to add or modify the key word searches?
- How will deduplication be handled?

- What format will the data take upon production? Will load files accompany the data? If so, what format is required? What fields will be in the load files?
- Can the parties agree to share the costs? Of the production? The same ediscovery vendor? A special master?
- How will the parties handle evidentiary issues at depositions and trial? Authenticity issues raised by the chain of custody? Hearsay?
- Who from each team will be designated as the liaison for e-discovery issues? Will technical personnel be allowed to directly communicate with each other?
- What is the timetable for collection and production in light of the need for depositions, expert designations, and trial?

The ultimate desire for the meet and confer is to determine the potential cost and need for the discovery of electronically stored information, and to determine if any extraordinary measure will be necessary.

Be specific in your conversation. For example, discuss how you are going to copy information. Some methods of copying can have implications on the metadata²⁸ associated with the information. This may not be an issue in your case; both sides may agree that no metadata or only certain metadata is necessary.

You will also want to decide what form your production will take. For example, will it be formatted for a litigation database? If so, who will pay the cost of transforming the data? Can the parties share a vendor?

At the end of your original meet and confer, it might be appropriate to enter into an agreement with respect to ESI and how it will be handled. Note the word "original." For the smooth handling of e-discovery, all parties should designate one lawyer from each team to continue to field any questions or concerns regarding continued production of electronic information.

^{28. &}quot;'Meta-Data' means: (i) information embedded in a Native File that is not ordinarily viewable or printable from the application that generated, edited, or modified such Native File; and (ii) information generated automatically by the operation of a computer or other information technology system when a Native File is created, modified, transmitted, deleted, or otherwise manipulated by a user of such system." Middle District of Maryland's *Suggested Protocol for Discovery of Electronically Stored Information*, www.mdd.uscourts.gov/sites/mdd/files/ESIProtocol.pdf, at 2–3.

I cannot stress the importance of meeting with the other side and reaching mutually beneficial agreements early in the case. You. Must. Cooperate.

If you cannot agree on a protocol for handling ESI, seek a conference with the Court. You may also be entitled to formal discovery on the way your opponent handles ESI. See chapter 6 of this book (Rule 26(f) Meet and Confer).

§ 5.9 Has My Client Properly Searched for, Preserved, and Produced Requested E-Mail?

This section depends greatly on the client and the type of case before you. In other words, some cases require more attention to e-mail messages than others. Some cases justify expending more money on locating and processing e-mail messages than others.

§ 5.9:1 Importance of E-Mail to a Particular Case

In order to efficiently describe the importance of e-mail to a particular case, one must first weigh the costs. My recommendation is to review the "Litigation Cost Survey of Major Companies" from the 2010 Conference on Civil Litigation presented to the Committee on Rules of Practice and Procedure Judicial Conference of the United States.²⁹

The following chart represents various types of civil suits and the typical importance or volume of e-mail. The chart moves from the types of cases that are most likely to involve high volumes of e-mail messages to those where e-mail messages may be less important.³⁰

^{29.} www.uscourts.gov/sites/default/files/litigation_cost_survey_of_major_companies_0.pdf.

^{30.} Federal Rule of Civil Procedure 26(b)(1) requires the parties to weigh the proportional value of requested discovery, including e-discovery. The Texas Supreme Court in *In re State Farm Lloyds*, 520 S.W.3d 595 (Tex. 2017), also demands that e-discovery should be reasonable in relation to the benefit to the case.

Type of Case	E-Mail Concerns
Intellectual property	Look for e-mails being forwarded to home or non-internal e-mail addresses
Antitrust; securities	Internal e-mails reviewing the market and attempting to corner it
Theft of trade secrets; noncompete; tortious interference	Look at accused user's personal e- mail traffic; synchronization files (if multiple devices are used); look for evidence of export to external devices
Products liability; consumer class action	Look for consumer complaints or correspondence with governmental entities (FDA, CPSC, NHTSA)
Malpractice	E-mails discussing related complaints or attempts to cover up
Employer/employee cases (termination, harassment, discrimination, embezzlement)	Look for deleted e-mails; e-mails sent to personal e-mail addresses
Family (divorce, child custody)	Inappropriate communications or evidence of abuse or mistreatment; also look at social media
Debt/contract	If contract is in dispute or unsigned, may need to look for e- mails that show the thought processes and understandings of the participants
Personal injury/workers' compensation	Likely to gain more information from social media (e.g., went out dancing last night while claiming in the lawsuit that they were too injured to work)

The type of case and the volume and importance of e-mail should drive the parties' agreements on the scope of e-mail discovery.

§ 5.9:2 Locating E-Mail

Simply assuming that e-mail resides only on the company's server and that all e-mail on the server has been properly purged according to the company's e-mail retention policy causes problems. See chapter 3 (Computer Usage Policies, Records Management & Information Governance). The location of e-mail depends on a number of factors, including the type of e-mail system (remember, different e-mail systems employ different protocols—once downloaded, certain protocols automatically purge that message from the server), user habits (some users will override company policy by forwarding "important e-mail" to their personal accounts or save information on thumb drives or other external media), hardware configuration (recall that some people access e-mail messages from multiple devices), and backup procedures.

Some questions that might be important:

- 1. What are the business and personal e-mail addresses for each potential witness?
- 2. What type of e-mail protocols do each of those e-mail addresses use?
- 3. What devices do each of these witnesses have to access e-mail?
- 4. Do different document retention habits pertain to different types of e-mail accounts?

By way of reference, the following places may hold relevant e-mail messages:

Location	Examples
File Server	Company-owned operating system—active e-mail server, archived e-mail, e-mail residing on former e-mail systems (for example, when a company changes its e-mail system from Lotus Notes to Outlook)
Computing Devices	Desktops, laptops, tablets, mobile phones; include those that have been traded in by a user to obtain a new device
External Backup Devices	Thumb drives, external hard drives

Location	Examples
Nonparty Servers	Gmail, iCloud, Yahoo, other cloud-based e-mail providers. This may be a source of e-mails that have been forwarded by a custodian from a business to a personal account. This could also include former e-discovery vendors if the client has been involved in other, similar litigation
Paper Printouts	Filing cabinets, off-site storage units, notebooks, etc.

§ 5.10 How Can I Best Mine E-Mail and Attachments to Further My Case?

Your approach to reviewing e-mails will depend entirely on the volume of e-mails expected and received in the litigation. It may be appropriate to simply review the e-mail messages in their native (original) system. For example, if e-mails were created and maintained in Outlook, the e-mail messages could be loaded onto a computer devoted to review in a dummy Outlook account. If the case involves voluminous e-mail messages, you may consider investing in an e-mail review platform, which provides a way to organize, notate, and sort documents in litigation.³¹

A document review platform allows the user to search and organize the produced information. It can show captured metadata. Common metadata fields that can be captured and produced to a review platform are:

^{31.} Since the original writing of this chapter, a host of new cloud-based review platforms have been created. This is an area of rapidly changing technology.

- Beginning Bates Number
- Ending Bates Number
- Beginning Attachment
- Ending Attachment
- Page Count
- Date Sent
- Time Sent
- Date Received
- Time Received
- Date Created
- Custodian
- То

- From
- CC
- BCC
- Subject
- Location
- Document Title
- File Extension
- Native Hash (a unique identifier of e-mail)
- Application
- Author
- Conversation Index
- Native Link

§ 5.11 Is This E-Mail Reliable Evidence?

E-mail is generally a reliable form of evidence, and most of the time the e-mails received are from exactly who they appear to be from. Unfortunately, much like U.S. mail and caller I.D., there are ways to "trick" the system and cause it to look like the message is coming from a trusted friend when it is actually a malicious e-mail or an attempt to pass an e-mail off as having certain traits that it does not have.³²

Just as there have always been questions about paper forgery, there is no way to prevent this type of abuse, because the wrongdoer does not need access to the e-mail account from which the e-mail originated, only the e-mail address. The user can examine the e-mail header information for some clues regarding the authenticity of the e-mail. The following are some ways to identify whether an e-mail is valid or trustworthy:

^{32.} For a further discussion of this topic, see chapter 18 of this book (Admissibility of ESI).

- Check the e-mail address. Although this is not a fail-safe method, sometimes the e-mail address is off by a single character or contains a misspelling.
- Look at the time and time zone. If the e-mail originated in a time zone other than the location where you know the sender resides, then that is an indicator that the sender of the e-mail may not be who you think it is.
- Examine the IP address, which can be found by searching the e-mail header, to track the path an e-mail message taken from the sender to the recipient.³³ An IP address is a series of numbers that is assigned to hardware (laptop, mobile phone, etc.) that is accessing the Internet. Each IP address is unique to the actual location from which the e-mail originated. Hardware can have differing IP addresses based upon how and where the connection is being made. For example, a laptop that is connected via an Ethernet cable at an office will have an IP address associated with the Internet at the office. But if you take that laptop to a location where it accesses the e-mail via public Wi-Fi, then it will be assigned a temporary IP address of the sender, and the IP address can then be used to track back to the physical location where the e-mail originated.

None of these tips are completely perfect. Experienced hackers have figured out methods to get around all of these preventative measures, but an amateur may not be sophisticated enough to trick the system. If the validity of the e-mail is denied by the purported sender, you may need to consult a technology expert.

Just because electronic data can be manipulated, it does not preclude its admissibility at trial. In *United States v. Safavian*, the court noted:

The possibility of alteration does not and cannot be the basis for excluding emails as unidentified or unauthenticated as a matter of course any more than it can be the rationale for excluding paper documents (and copies of those documents). We live in an age of technology and computer use where email communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance in the professional world. The defendant is free to raise this issue with the jury and put on evidence that emails are capable of being altered before they are

^{33.} The following website gives step-by-step instructions to access the header information on the most popular webmail providers and e-mail clients: https://support.google.com/mail/answer/ 22454?hl=en.

passed on. Absent specific evidence showing alteration, however, the Court will not exclude embedded emails because of the mere possibility that it can be done.³⁴

Because of its increasing popularity, e-mail is becoming more interwoven into lawsuits. Therefore, it is important to identify and analyze the admissibility of e-mails at the earliest possible phase of the litigation. Because of the cost of employing a technology expert, it is recommended that counsel cooperate and obtain agreements with opposing counsel regarding the authenticity and admissibility of e-mails produced in litigation.

§ 5.12 Conclusion

Understanding e-mail messages, how they work, and their history helps lawyers locate, preserve, produce, and use what may be the most important evidence in a case. It also assists lawyers in discharging their ethical duty to efficiently and effectively represent their clients in today's world. Just remember my words of wisdom: Cooperate! Cooperate! Cooperate!

34. 435 F. Supp. 2d 36, 41 (D.D.C. 2006), rev'd on other grounds, 528 F.3d 957 (D.C. Cir. 2008).

Chapter 6

Rule 26(f) Meet and Confer

Ramona L. Lampley¹

§ 6.1 Introduction

The "meet and confer" requirement of rule 26(f) of the Federal Rules of Civil Procedure is a bit like performing the tango—the choreography requires the partners to take long pauses in seemingly difficult positions.² This rings particularly true if a party faces overwhelming e-discovery requests and has not adequately prepared for or participated in the rule 26(f) conference. Rule 26(f)'s requirement that the parties meet to discuss the case in its initial stages is not new. It has long required that the parties meet to discuss the nature and basis of their claims and defenses, the possibilities of prompt settlement or case resolution, and to arrange or make initial disclosures.³ But the 2006 amendments added a critical component to this discussion.⁴ Parties must discuss "issues about disclosure, discovery, or preservation of electronically stored information" ("ESI").⁵ Rule 26(f) applies "[e]xcept in a proceeding exempted from initial disclosure[s] under Rule 26(a)(1)(B) or when the court orders otherwise[.]"⁶

^{1.} Thank you to David Kessler and Professor Albert Kauffman for their contributions to this chapter. My thanks are also due to Judge Xavier Rodriguez for this opportunity to comment on this important area of developing law. Finally, I owe a special Thank You to my diligent research assistants Leigh Ann Woitena, Christopher Chaffee, and Lindsey LacIli for their thoughtful comments and tireless editing.

^{2.} Merriam-Webster's dictionary defines the "tango" as a "ballroom dance of Latin-American origin in 2/4 time with a basic pattern of step-step-step-close and characterized by long pauses and stylized body positions" or as "interaction marked by a lack of straightforwardness."

^{3.} Fed. R. Civ. P. 26(f). The rule 26(f) concept was first established by the 1980 amendments to the Federal Rules of Civil Procedure and was primarily put in place to curb "widespread criticism of abuse of discovery." Fed. R. Civ. P. 26 advisory committee's note (1980). These discovery meetings became mandatory with the 1993 amendments unless a local rule provided otherwise. The 2000 amendments to rule 26(f) made the meet and confer requirement mandatory by removing the local rules provision. Fed. R. Civ. P. 26 advisory committee's note (2000).

^{4.} Rule 26(f)(3) was amended in 2015 to add two items to the discovery plan: issues about preserving electronically stored information and court orders under Federal Rule of Evidence 502. But the 2006 amendments, though over 12 years ago, remain the watershed amendments for the purpose of this chapter.

^{5.} Fed. R. Civ. P. 26(f)(3)(C).

^{6.} Fed. R. Civ. P. 26(f)(1).

This chapter only addresses the requirements for the meet and confer meeting(s) pursuant to Federal Rule of Civil Procedure 26. While Texas has not adopted identical language patterning the 2006 amendments to the federal rules, in *In re Weekley Homes, L.P.*, the Texas Supreme Court stated:

[A] fundamental tenet of our discovery rules is cooperation between parties and their counsel, and the expectation that agreements will be made as reasonably necessary for efficient disposition of the case. Tex. R. Civ. P. 191.2. Accordingly, prior to promulgating requests for electronic information, parties and their attorneys *should share relevant information concerning electronic systems and storage methodologies so that agreements regarding protocols may be reached* or, if not, trial courts have the information necessary to craft discovery orders that are not unduly intrusive or overly burdensome. The critical importance of learning about relevant systems early in the litigation process is heavily emphasized in the federal rules. Due to the "volume and dynamic nature of electronically stored information," failure to become familiar with relevant systems early on can greatly complicate preservation issues, increase uncertainty in the discovery process, and raise the risk of disputes.⁷

Thus, the Texas Rules of Civil Procedure draw heavily on guidance from the Federal Rules of Civil Procedure, including instructions regarding rule 26(f).

§ 6.2 Nuts and Bolts of Rule 26(f)

The following provides an at-a-glance overview of the "nuts and bolts" of rule 26(f)'s requirements.

§ 6.2:1 When Must the Conference Take Place?

As "soon as practicable" and "at least 21 days before a scheduling conference is to be held or a scheduling order is due under rule 16(b)."⁸ But as discussed in this chapter, the rule 26(f) meet and confer concept is an iterative process and may require multiple meetings throughout the case.

^{7.} In re Weekley Homes, L.P., 295 S.W.3d 309, 321–22 (Tex. 2009) (orig. proceeding) (emphasis added) (citing Fed. R. Civ. P. 26(f) advisory committee's note to the 2006 amendments).

^{8.} Fed. R. Civ. P. 26(f)(1). Of course, in my experience, some parties will convene a rule 26(f) conference to simply discuss delaying the time of the conference, a tactic that flies in the face of the spirit of the rule.

§ 6.2:2 Who Must Attend the Conference?

The attorneys of record and any unrepresented parties must attend the conference.⁹ Although many rule 26(f) conferences do not take place in person, the court can require it.¹⁰ Further, meeting in person may make it more likely that the parties will reach an agreement on some matters. Amended in 2015, Federal Rule of Civil Procedure 1 provides that the rules "should be construed, administered, and employed by the court *and the parties* to secure the just, speedy, and inexpensive determination of every action and proceeding."¹¹ Consistent with rule 1, rule 26(f)(3) puts the burden on the parties to prepare, identify issues with ESI discovery, and to cooperate.

§ 6.2:3 What Must Be Discussed?

At the conference, the issues that must be discussed include—

- 1. the nature and basis for the claims and defenses;
- 2. the possibilities of promptly settling or resolving the case;
- 3. making or arranging for initial disclosures required by rule 26(a)(1);
- 4. any issues about preserving discoverable information; and
- 5. a proposed discovery plan.¹²

§ 6.2:4 Proposed Discovery Plan

The parties bear joint responsibility "for arranging the conference, for attempting in good faith to agree on the proposed discovery plan," and for developing the proposed discovery plan.¹³ What must be included in the proposed discovery plan, and how does that bear on the issue of ESI?

In 2015, the federal rules were amended to permit early delivery of rule 34 requests for production (RFP) such that they can now be delivered (not served) prior to the rule 26(f) conference for the parties' discussion.¹⁴ Rule 26(d)(2) permits delivery twenty-

- 9. Fed. R. Civ. P. 26(f)(2).
- 10. Fed. R. Civ. P. 26(f)(2).
- 11. Fed. R. Civ. P. 1 (emphasis added).
- 12. Fed. R. Civ. P. 26(f)(2).
- 13. Fed. R. Civ. P. 26(f)(2).
- 14. Fed. R. Civ. P. 26(d)(2) (2015 amendment).

one days after service of process. The RFPs are deemed served as of the date of the rule 26(f)(3) process, which starts the ticking of the thirty-day clock.¹⁵ This change was designed to facilitate early discussion about ESI requested.¹⁶

Rule 26(f) must be read in conjunction with its counterpart—Federal Rule of Civil Procedure 16. Pursuant to rule 16, the judge must issue a scheduling order after receiving the parties' rule 26(f) report or after consulting with the parties' attorneys and unrepresented parties.¹⁷ The scheduling order will likely reflect any agreements reached by the parties in the rule 26(f) conference that are adopted by the presiding judge.¹⁸ Understanding what must be discussed at a rule 26(f) conference with respect to ESI for any particular case begins with understanding the purposes of the 2006 amendments: "When the parties do anticipate disclosure or discovery of electronically stored information, discussion at the outset may avoid later difficulties or ease their resolution."¹⁹ Thus, the goal of the conference and counsel's obligations to cooperate is to avoid late-arising discovery disputes and increased costs due to the failure to foresee a potential problem. The discovery plan requires that the parties address the following, with the ESI-specific components underlined:²⁰

- Changes to "the timing, form, or requirement for" initial disclosures, "including a statement of when" the initial disclosures will be made.²¹
- "[S]ubjects on which discovery may be needed;"²² whether discovery should be phased,²³ and when discovery should be completed.²⁴

17. Fed. R. Civ. P. 16(b)(1) (local rules may exempt some actions).

18. See Fed. R. Civ. P. 16(b)(3)(B)(iii–iv) (permitting scheduling order to "provide for disclosure, discovery, or preservation of electronically stored information" and "include any agreements the parties reach for asserting claims of privilege").

19. Fed. R. Civ. P. 26(f) advisory committee's note (2006).

20. By now it should be apparent that it is impossible to discuss the production of ESI in a vacuum. It would be a mistake to try to tackle only the form of production of ESI without first discussing the nature and basis of the parties' claims and defenses, or the subjects on which discovery should be made. See Fed. R. Civ. P. 26(f)(2)–(3).

21. Fed. R. Civ. P. 26(f)(3)(A).

22. Fed. R. Civ. P. 26(f)(3)(B).

^{15.} Fed. R. Civ. P. 26(d)(2) (2015 amendment).

^{16.} The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production,* 19 Sedona Conf. J. 1, Principle 3, at 72 (2018), *available at* https://thesedonaconference.org/publication/The_Sedona_Principles. The Sedona Conference is a "nonprofit 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights." The Sedona Conference, About the Sedona Conference, https://thesedonaconference.org. It has generated valuable publications in the area of e-discovery that are widely relied on by judges and lawyers.

- "[A]ny issues about disclosure, discovery, or preservation of [ESI]."²⁵ This should include whether any form of ESI is "not reasonably accessible because of undue burden or cost."²⁶
- "[T]he form or forms in which" ESI is to be produced.²⁷
- Issues regarding claims of privilege or protection of "trial-preparation materials" (work product), including whether to ask the court to include any agreements reached on procedure for asserting these claims after inadvertent production (for example, clawback agreements).²⁸
- What changes should be made in discovery limitations imposed by the Federal Rules of Civil Procedure or by local rule, and whether other limitations should be imposed.²⁹
- "[A]ny other orders the court should issue under" rule 26(c) (Protective Orders) or rule 16(b) (Scheduling) and (c) (Pretrial Conference).³⁰

Additionally, while not explicitly mandated by the federal rules, The Sedona Conference observes that "an obligation to discuss ESI issues as early as practicable and in good faith also applies to nonparties from whom information is sought under Rule 45."³¹

25. Fed. R. Civ. P. 26(f)(3)(C).

26. Fed. R. Civ. P. 26(f)(3)(B). *See also* The Sedona Conference, *The Sedona Principles*, Principle 3, at 71 ("As soon as practicable, parties should confer and seek to reach agreement regarding the preservation and production of [ESI].").

27. Fed. R. Civ. P. 26(f)(3)(C).

28. Fed. R. Civ. P. 26(f)(3)(D). Rule 26(b)(5)(B) sets forth the clawback provision adopted by the federal rules. See chapter 10 of this book. Its basic requirements are that for information produced (one would assume inadvertently) that is subject to a claim of privilege or work product protection, the party asserting the claim may notify any party receiving the information of the claim and the basis for the claim. The receiving party must then "promptly return, sequester, or destroy" the specified information and any copies, must not use the information, and must take reasonable steps to retrieve the information if it has already been disclosed. Fed. R. Civ. P. 26(b)(5)(B). If the receiving party contests the privilege or work product assertion, he or she may present it "to the court under seal for a determination" of the issue. Fed. R. Civ. P. 26(b)(5)(B); *see also* Fed. R. Evid. 502.

29. Fed. R. Civ. P. 26(f)(3)(E).

30. Fed. R. Civ. P. 26(f)(3)(F).

31. The Sedona Conference, The Sedona Principles, Principle 3, at 74.

^{23.} For example, in a products case in which the manufacturer is not certain, the first phase may involve discovery as to product identification. Alternatively, discovery may be split between an initial phase for fact discovery followed by expert discovery, depending on the complexity of the case. See Fed. R. Civ. P. 26(f)(3)(B).

^{24.} Fed. R. Civ. P. 26(f)(3)(B).

Thus, it has been said that rule 26(f) requires the parties to discuss the three P's of ESI: production, privilege, and preservation.³² This chapter addresses each component, then proposes additional topics for discussion and follows with some pointers on how to prepare for the rule 26(f) conference.

§ 6.3 Form of Production

An essential component of the rule 26(f) conferences is that the parties should attempt to come to an agreement on the form of production.³³ "Form of Production" may refer both to "file format (for example, native vs. imaged format) and the media on which the documents are produced (paper vs. electronic);"³⁴ and the methodology for document sweeps and production, including the potential use of search technology.³⁵

Before the parties can come to an educated agreement as to form or forms of production, the parties should have a reasonable idea of the subject matter of the discovery sought and the form in which it is usually held in the ordinary course of business. Rule 34(b) outlines a procedure for reaching agreement on the form or forms of production of ESI, and, if no agreement is specified, the responding party must produce ESI "either in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable."³⁶ The most common file formats used in production are: TIFF, PDF, and native format.³⁷ The technical definitions of each of these formats are:

TIFF (Tagged Image File Format): A widely used and supported graphic file format for storing bitmapped images, with many different compression

^{32.} Ronald J. Hedges, "The ESI Amendments to the Federal Rules of Civil Procedure: A Rule-By-Rule Look," *in Managing E-Discovery and ESI: From Pre-Litigation Through Trial* 35–36 (Michael D. Berman et al. eds., 2011).

^{33.} Fed. R. Civ. P. 26(f) advisory committee's note (2006) ("Early identification of disputes over the forms of production may help avoid the expense and delay of searches or productions using inappropriate forms."); *see also* The Honorable Xavier Rodriguez, Scheduling and Docket Control Order, at § 2.06, *available at* http://www.txwd.uscourts.gov/Rules/StandingOrders/SanAntonio/sched_xr.pdf (requiring counsel or the parties to make a "good faith" effort "to agree on the format(s) for production of ESI (whether native or some other reasonably usable form)"). Judge Rodriguez's protocol specifies that the requesting party is generally responsible for the "cost of creating its copy of" the requested information and encourages early discussion of cost-sharing "for optical character recognition (OCR) or other upgrades" to "paper documents or non-text-searchable electronic images[.]."

^{34.} The Sedona Conference, *The Sedona Conference Glossary: E-Discovery & Digital Information Management (Fourth Edition)*, 15 Sedona Conf. J., at 328 (2014), *available at* https://thesedonaconference.org/publication/The_Sedona_Conference_Glossary.

^{35.} See The Sedona Conference, The Sedona Principles, Principle 3, at 72.

^{36.} Fed. R. Civ. P. 34 advisory committee's note (2006).

formats and resolutions. File name has .TIF extension. Can be black and white, gray-scale, or color. Images are stored in tagged fields, and programs use the tags to accept or ignore fields, depending on the application.

PDF (Portable Document Format): A file format technology developed by Adobe Systems to facilitate the exchange of documents between platforms regardless of originating application by preserving the format and content.³⁸

Native Format: Electronic documents have an associated file structure defined by the original creating application. This file structure is referred to as the native format of the document. Because viewing or searching documents in the native format may require the original application (for example, viewing a Microsoft Word document may require the Microsoft Word application), documents may be converted to a neutral format as part of the record acquisition or archive process. . . . It should be noted that not all ESI may be conducive to production in either the Native Format or imaged format, and some other form of production may be necessary. Databases, for example, often present such issues.³⁹

Some ESI is more suitable for production in imaged forms, such as e-mail, memoranda, image files or basic presentations.⁴⁰ If this information is ordinarily maintained in a way that makes it searchable by electronic means, the parties should agree on a form that preserves the electronically searchable feature.⁴¹ These imaged formats are typically accompanied by "load files," for example, ancillary files containing textual

41. Fed. R. Civ. P. 34 advisory committee's note (2006).

^{37.} Judge David J. Waxse, *The Technology and Law of the Form of Production of Electronically Stored Information*, Judges' J. at 33, 35 (Summer 2010). Although there is no need to produce a responsive document in multiple forms, Fed. R. Civ. P. 34 advisory committee's note (2006), the form of production may vary depending on the nature of the ESI. See Craig Ball, *E-Discovery: A Special Master's Perspective*, 51 The Advocate 42, 44 (State Bar of Texas 2010) ("Counsel often don't grasp the importance of specifying the forms of production sought or mistakenly assume that they must select one form to be applied to all production. One size doesn't fit all.").

^{38.} The Sedona Conference, The Sedona Conference Glossary, at 347.

^{39.} The Sedona Conference, The Sedona Conference Glossary, at 341.

^{40.} Ball, *E-Discovery*, at 44. ("Some ESI lends itself to paper-like forms. For example, e-mail remains reasonably usable when produced as searchable images (i.e., Adobe PDF files or TIFF images accompanied by load files holding searchable text and metadata). But other ESI, such as formulae underlying spreadsheet cells, animated presentations or contents of databases, require forms of production closer or identical to the native forms used by the producing party."); Thomas Y. Allman, *Managing Preservation Obligations After the 2006 Federal E-Discovery Amendments*, 13 Rich. J.L. & Tech. 9, 31 (2007) ("Parties frequently agree to produce e-mail in convenient and difficult to alter forms that faithfully preserve the appearance of the content so that the images of individual pages can be Bates numbered and readily used in depositions and at trial.").

content and relevant metadata.⁴² Other ESI may necessitate a form of production that is native, or near-native, so that the receiving party can actually utilize the information.⁴³ This might include spreadsheets, particularly if one is interested in the formulas used, animations, or databases.⁴⁴ The parties should also work to make sure that the form of production (format and media) is compatible with the tools one has to conduct the review. Receiving a database in native format, for example, is of little use if one does not have the program necessary to run it.⁴⁵ The advisory committee notes to rule 34 contemplate that in some circumstances the producing party may need to provide some "reasonable amount of technical support, information on application software, or other reasonable assistance to enable the requesting party to use the information."46 Failure to communicate—and agree—early in the case on the appropriate form of production may result in a party facing reproduction of discovery already reviewed and produced or further sanctions. In Covad Communications Co. v. Revonet, Inc., the court ordered reproduction of e-mails in native format that had originally been converted to hard copy and produced as such.⁴⁷ The court ordered that the parties share the costs of having a paralegal remove privileged e-mails from the production set and advised that "courts have reached the limits of their patience with having to resolve electronic discovery controversies that are expensive, time consuming, and so easily avoided by the lawyers' conferring with each other on such a fundamental question as the format of their productions of electronically stored information."48

^{42.} Allman, Managing Preservation Obligations, at 31. See also Aguilar v. Immigration & Customs Enforcement Div. of U.S. Dep't of Homeland Sec., 255 F.R.D. 350, 356 (S.D.N.Y. 2008) (concluding that "even if native files are requested, it is sufficient to produce memoranda, emails, and electronic records in PDF or TIFF format accompanied by a load file containing searchable text and selected metadata" (citing The Sedona Conference, *The Sedona Principles*, cmt. 12b illus. i)).

^{43.} Covad Communications Co. v. Revonet, Inc., 260 F.R.D. 5, 9 (D.D.C. 2009) (chastising production of spreadsheets in hard copy by stating, "taking an electronic document such as a spreadsheet, printing it, cutting it up, and telling one's opponent to paste it back together again, when the electronic document can be produced with a keystroke is madness in the world in which we live").

^{44.} From the producing party's standpoint, native format poses some issues, none of which are insurmountable. The native files may be difficult or impossible to redact Bates number or use in deposition or trial. How might one quote or reference a native file in a motion? The parties will also want to ensure that the reviewer does not corrupt the information in the native file. The native file format may complicate the privilege review. If native format is contemplated, the parties should strive to reach agreement on these additional burdens associated with native file production. *See, e.g.*, Allman, *Managing Preservation Obligations*, at 28 n.84.

^{45.} See Allman, Managing Preservation Obligations, at 28 n.84. Craig Ball advises that if requesting native file formats, the review platform must be able to open the various types of data received without corrupting its content or metadata.

^{46.} Fed. R. Civ. P. 34 advisory committee's note (2006).

^{47. 254} F.R.D. 147, 151 (D.D.C. 2008).

^{48.} Covad Communications, 254 F.R.D. at 151.

Another issue that should be addressed in the rule 26(f) conference is the production (or nonproduction) of metadata and embedded data. The advisory committee distinguished between embedded data and metadata:

For example, production may be sought of information automatically included in electronic files but not apparent to the creator or to readers. Computer programs may retain draft language, editorial comments, and other deleted matter (sometimes referred to as "embedded data" or "embedded edits") in an electronic file but not make them apparent to the reader. Information describing the history, tracking, or management of an electronic file (sometimes called "metadata") is usually not apparent to the reader viewing a hard copy or a screen image.⁴⁹

As Magistrate Judge Frank Maas said in 2008, "Metadata has become 'the new black,' with parties increasingly seeking its production in every case, regardless of size or complexity."⁵⁰ Some courts have recognized that "the more interactive the application, the more important the metadata" is to using the application's output.⁵¹ Before the 2006 amendments, the Sedona Conference took the position that metadata need not be produced unless it bore some material relevance to the dispute.⁵² But the 2006 amendments to the Federal Rules contemplated the production of embedded data or metadata in certain cases, without giving any indication as to when such production should be required.⁵³ Following these amendments, Sedona Principle 12 was revised to provide "a more neutral view of the need for metadata."⁵⁴ Sedona Principle 12 now reads, "The production of electronically stored information should be made in the form or forms in which it is ordinarily maintained or that is reasonably usable given the nature of the electronically stored information and the proportional needs of the case."⁵⁵

52. The pre-2006 amendment Sedona Principles provide that "[u]nless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court." The Sedona Conference, *The Seaona Principles*.

^{49.} Fed. R. Civ. P. 26(f) advisory committee's note (2006). For example, the date a document was created or modified is metadata. For a discussion of the different types of metadata that may be at issue in a particular case, see *Aguilar*, 255 F.R.D. at 354.

^{50.} Aguilar, 255 F.R.D. at 359.

^{51.} Aguilar, 255 F.R.D. at 353–54 (noting that "[a] spreadsheet application lies somewhere in the middle' and the need for its metadata depends upon the complexity and purpose of the spreadsheet") (quoting *Williams v. Sprint/United Management Co.*, 230 F.R.D. 640, 647 (D. Kan. 2005)).

^{53.} Fed. R. Civ. P. 26(f) advisory committee's note (2006) ("[P]roduction may be sought of information automatically included in electronic files but not apparent to the creator or to readers." (discussing metadata and embedded data)).

^{54.} Waxse, The Technology and Law, at 33, 36.

Thus, the third edition of *The Sedona Principles* seems to focus more on the accessibility and functionality to receiving parties.⁵⁶ Since the 2006 amendments, the failure of a party to request metadata in the rule 26(f) conference has led some courts to refuse to order the reproduction of discovery with metadata (once the party finally requested it) or to order the late requesting party to pay the costs of reproduction.⁵⁷ Beyond these basic considerations, the highly explosive variety of forms of ESI will merit some thoughts as to production and preservation. These include text messages, group chats, social media pages, and information stored on the cloud.

Courts continue to struggle with whether production in native format is necessary, but the federal rules permit the requesting party to specify the format of production. For example, in Morgan Hill Concerned Parents Ass'n v. California Department of Education,⁵⁸ the plaintiffs moved to compel the defendant to produce e-mails in "native" format with all metadata attached. The plaintiffs first set of requests for production specified that "ESI should be produced 'in their native electronic format together with all metadata and other information associated with each document in its native electronic format.""59 The California Department of Education (CDE) did not initially object to the requested form of production, but produced the e-mails in an "industry standard load format."60 CDE later argued that "[a] requesting party cannot demand production in one format versus another just because one would allegedly ease a party's review process."⁶¹ The court rejected that argument stating: "This argument runs directly contrary to the governing Rules, which expressly state just the opposite: the requester 'may specify the form or forms in which electronically stored information is to be produced."62 "The Rule does not limit this authorization to any specific set of circumstances, nor does it say that specifying the format is not available to 'ease' the review process. Indeed, CDE's dismissive rejection of 'ease' of review as a

- 59. Morgan Hill, 2017 WL 445722, at *2.
- 60. Morgan Hill, 2017 WL 445722, at *1.
- 61. Morgan Hill, 2017 WL 445722, *4.
- 62. Morgan Hill, 2017 WL 445722, at *4 (quoting Fed. R. Civ. P. 34(b)(1)(C)).

^{55.} The Sedona Conference, The Sedona Principles, at 169 (emphasis added).

^{56.} See Aguilar, 255 F.R.D. at 354.

^{57.} Aguilar, 255 F.R.D. at 360, 362 (denying motion to order discovery of e-mails with metadata when the requesting party failed to request metadata before the document collection, and ordering the plaintiffs to pay the costs of reproduction of word processing and PowerPoint documents with metadata for failure to request prior to document collection); *Chevron Corp. v. Stratus Consulting, Inc.*, No. 10-cv-00047-MSK-MEH, 2010 WL 3489922, at *2–4 (D. Colo. Aug. 31, 2010) (ordering the requesting party to pay costs of reproducing discovery with metadata when the party failed to make clear that its request encompasses metadata in the specified format).

^{58.} No. 2:11-CV-3471 KJM AC, 2017 WL 445722, at *1 (E.D. Cal. Feb. 2, 2017).

valid reason for specifying the format is difficult to understand, since ease of review is precisely why the requesting party would specify the format, and it is the very reason the requester is permitted to do so."⁶³ The defendant also argued that it would be burdensome to require it to "reproduce" ESI in native format. The court rejected "this argument because this is a problem of CDE's own making. CDE created the problem it now complains about by engaging in an ESI production in a format of its choosing—the 'load file format'—rather than the native format, with all metadata attached, as plaintiffs had requested."⁶⁴ Note that this is a dispute that could have been entirely avoided had the parties agreed prior to production on the form of production.

For a somewhat different view at the state level, in *In re State Farm Lloyds* the Texas Supreme Court applied the Tex. R. Civ. P. 192.4 proportionality factors to a request for production that specified a "native" format for production.⁶⁵ It remanded the case to the trial court to "assess whether any enhanced burden or expense associated with a requested form is justified when weighed against the proportional needs of the case."⁶⁶ State Farm argued that its static form was adequate, and it produced the requested documents as they were kept in the ordinary course of business. The plain-tiffs sought some of the static form data (primarily photographs and related data) in their native format to capture what they believed was relevant metadata.

§ 6.4 Preservation

One of the most straightforward ways to avoid discovery disputes and ease the financial burden of preservation on the parties is for the parties to agree at the outset of litigation on the scope of preservation. The advisory committee to the 2006 amendments to the Federal Rules of Civil Procedure recognized that "[f]ailure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes."⁶⁷ One way to limit the parties' duty to preserve is for the parties to agree on a date range for potentially relevant ESI based on the nature of claims and defenses. ESI outside of the agreed on date range need not be preserved. The advisory committee notes direct the parties to "pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities."⁶⁸ Thus, "[c]omplete or broad cessation of a party's routine computer oper-

^{63.} Morgan Hill, 2017 WL 445722, at *4.

^{64.} Morgan Hill, 2017 WL 445722, at *7 (emphasis in original).

^{65. 520} S.W.3d 595 (Tex. 2017).

^{66.} In re State Farm Lloyds, 520 S.W.3d at 607.

^{67.} Fed. R. Civ. P. 26(f) advisory committee's note (2006).

ations could paralyze the party's activities."⁶⁹ The goal at all times is to agree on "reasonable" preservation steps.⁷⁰

The *Manual for Complex Litigation*, a publication by the Federal Judicial Center for judges, includes a sample case management order on "Preservation of Documents, Data, and Tangible Things."⁷¹ This order directs the parties to attempt to reach an agreement on the following preservation issues:

- (a) the extent of the preservation obligation, identifying the types of material to be preserved, the subject matter, time frame, the authors and addressees, and key words to be used in identifying responsive materials;
- (b) the identification of persons responsible for carrying out preservation obligations on behalf of each party;
- (c) the form and method of providing notice of the duty to preserve to persons identified as custodians of documents, data, and tangible things;
- (d) mechanisms for monitoring, certifying, or auditing custodian compliance with preservation obligations;
- (e) whether preservation will require suspending or modifying any routine business processes or procedures, with special attention to document-management programs and the recycling of computer data storage media;
- (f) the methods to preserve any volatile but potentially discoverable material, such as voicemail, active data in databases, or electronic messages;
- (g) the anticipated costs of preservation and ways to reduce or share these costs; and

^{68.} Fed. R. Civ. P. 26(f) advisory committee's note (2006).

^{69.} Fed. R. Civ. P. 26(f) advisory committee's note (2006).

^{70.} Fed. R. Civ. P. 26(f) advisory committee's note (2006).

^{71.} Federal Judicial Center, *Manual for Complex Litigation, Fourth*, § 40.25 (2004). This sample order listing topics for discussion in a meet and confer was cited by the advisory committee in the notes to the 2006 amendments to rule 26(f).
(h) a mechanism to review and modify the preservation obligation as discovery proceeds, eliminating or adding particular categories of documents, data, and tangible things.⁷²

Depending on the nature of the case, some of these topics will be more critical to the rule 26(f) discussion than others. For example, in any case that will require preservation of ESI, the parties should attempt to agree on the time frame for preservation, the subject matter, and key custodians. They should also address whether preservation will require suspending or modifying any routine business processes, such as document retention policies. Whether identification of the person responsible for carrying out preservation obligations, and a discussion of the form and method of providing notice to custodians of documents is something that should be addressed depends on the needs of the case.⁷³

To facilitate an informed discussion on the preservation methods and anticipated costs, it is important for the parties to ciscuss their information systems with opposing counsel, and "for counsel to become familiar with those systems before the conference."⁷⁴ One of the most expensive components of preservation is preserving backup media.⁷⁵ The report of the civil rules committee described backup media as an example of an inaccessible source because it is "often not indexed, organized, or susceptible to electronic searching."⁷⁶ While there are reported cases in which sanctions have been given for failure to preserve backup tapes, the Sedona Principles suggest that preservation obligations should not extend to backup media "absent special circumstances."⁷⁷ One way in which the parties could compromise to alleviate the burden and expense of retaining all backup tapes is to retain the most recent backup along with select copies from relevant time periods.⁷⁸ Once these backup tapes are with-

74. Fed. R. Civ. P. 26(f) advisory committee's note (2006).

75. See Allman, Managing Preservation Obligations, at 41 n.121 ("Large organizations often recycle hundreds of backup tapes every two or three weeks and placing a litigation hold on recycling can result in large expenses if the holds are maintained even for a short period of time."); see also The Sedona Conference, *The Sedona Principles*, Comment 5.h., at 35. Backup tapes allow recovery of information, a "snapshot" of data at a given point in time, in the event of loss or disaster and are typically recycled and overwritten pursuant to routine document retention policies. Allman, Managing Preservation Obligations, at 40–41.

76. Allman, *Managing Preservation Obligations*, at 41 n.121 (citing report of the civil rules advisory committee (July 25, 2005) at *1127).

77. Allman, *Managing Preservation Obligations*, at 41; The Sedona Conference, *The Sedona Principles*, Principle 5, Comment 5.h., at 112.

^{72.} Federal Judicial Center, Manual for Complex Litigation § 40.25.

^{73.} Typically, the issuance of a litigation hold and ensuring compliance with preservation efforts is a topic handled between counsel and client, with no input or interference from the other party. Advance agreement as to these issues can head off any future disputes regarding failure to preserve.

§ 6.4

drawn from the routine recycling program, normal procedures could be reinstated.⁷⁹ The recycling of future backup media should not normally be halted because alternative methods of preserving information, if effectively implemented, should be sufficient. Indeed, the advisory committee suggested that early and practical agreement is the best remedy for avoiding the quandary between expensive preservation of backup tapes and the risk of sanctions for failure to preserve.⁸⁰ If the case involves the need to preserve or produce dynamic information that is constantly overwritten, more creative solutions will be necessary. For example, one author suggests that for database information in which results are desired, the parties "work out an arrangement, by agreement or court order, whereby agreed-upon queries of the database are made and recorded. The results may be saved in imaged format^{**1} This method preserves the data requested but does not require impeding the usefulness of the database.

§ 6.5 Privilege

The third major component that must be addressed in the rule 26(f) conference pertains to assertions of privilege or work production protection. Parties should attempt to agree on a procedure for the assertion of these claims to encourage the efficacy of litigation and the discovery process.⁸² The advisory committee specifically noted that one of the goals of the conference is to avoid the burden and expense of extensive and timely privilege review.⁸³ The committee stated that "[f]requently parties find it necessary to spend large amounts of time reviewing materials requested through discovery to avoid waiving privilege. . . . [and] [p]arties may attempt to minimize these costs and delays by agreeing to protocols that minimize the risk of waiver."⁸⁴ The advisory committee went on to suggest two possible ways of minimizing this risk: (1) the "quick peek," in which the responding party provides requested materials for an initial examination without waiving any privilege or protection and the requesting party then

- 81. Allman, Managing Preservation Obligations, at 48.
- 82. Fed. R. Civ. P. 26(f) advisory committee's note (2006).
- 83. Fed. R. Civ. P. 26(f) advisory committee's note (2006).
- 84. Fed. R. Civ. P. 26(f) advisory committee's note (2006).

^{78.} Allman, Managing Preservation Obligations, at 41.

^{79.} See, e.g., In re Celexa and Lexapro Products Liability Litigation, No. MDL 1736, 2006 WL 3497757, at *2 (E.D. Mo. Nov. 13, 2006) (designating thirty-five backup tapes to be preserved but permitting the defendants to otherwise resume recycling backup tapes).

^{80.} Fed. R. Civ. P. 26(b)(2)(B) advisory committee's note (2006) ("Whether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible depends on the circumstances of each case. It is often useful for the parties to discuss this issue early in discovery.").

designates the documents it wishes to actually have produced (which are then produced after privilege review), and (2) "clawback agreements," in which inadvertent production does not result in a waiver as long as the responding party identifies the document mistakenly produced and the document is returned.⁸⁵ To add some strength to the proposed antiwaiver agreement reached by the parties, rule 26(f) permits the court to include any such agreement in a case-management order.⁸⁶ Federal Rule of Evidence 502 includes its own antiwaiver provision; if the disclosure is inadvertent, the holder takes reasonable steps to prevent disclosure and the holder takes reasonable steps to rectify the error.⁸⁷ But parties to the rule 26(f) conference can modify this rule to fit the needs of their case by modifying or defining what is "reasonable" to prevent disclosure. Additionally, parties could agree that if a receiving party obtains inadver-

tently produced information, it will notify the producing party of the inadvertent production.⁸⁸

The parties may also want to discuss methods for modifying production of a privilege log to ease the costs associated with its creation and how to redact privileged information from ESI and protect metadata that is to be produced.⁸⁹ Magistrate Judge Love chastised the parties in *SmartPhone Technologies LLC. v. Apple, Inc.* for failing to confer on production of privilege logs as required by rule 26(f) and the discovery and docket control orders.⁹⁰ The court stated that "[s]uch a course of conduct disregarded an explicit obligation" of the parties.⁹¹

§ 6.6 What Else Might Be Addressed at the Rule 26(f) Conference?

Once the parties have addressed the main components of the discovery plan outlined above, the potential for reaching agreement (or raising early issues of nonagreement) on other issues can be tailored to the facts of the specific case.

^{85.} Fed. R. Civ. P. 26(f) advisory committee's note (2006).

^{86.} See Fed. R. Civ. P. 26(f) advisory committee's note (2006) ("Although these agreements may not be appropriate for all cases, in certain cases they can facilitate prompt and economical discovery by reducing delay before the discovering party obtains access to documents, and by reducing the cost and burden of review by the producing party.").

^{87.} Fed. R. Evid. 502.

^{88.} Michael D. Berman, "The Rule 26(f) Conference of the Parties," *in Managing E-Discovery and ESI: From Pre-Litigation Through Trial* 421, 429 (Michael D. Berman et al. eds., 2011).

^{89.} Berman, "The Rule 26(f) Conference of the Parties," at 428.

^{90.} No. 6:10cv74 LED-JDL, 2013 WL 789285, at *4 (E.D. Tex. Mar. 1, 2013).

^{91.} SmartPhone Technologies, 2013 WL 789285, at *2.

§ 6.6:1 Admissibility

One thing the parties should consider before expending the time and expense to perform extensive ESI document collections, production, and review is the admissibility of the ESI requested. As one court noted,

[C]onsidering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted.⁹²

The parties should ensure that the agreed-on production format or collection efforts do not degrade the authenticity of the information.⁹³ If the parties agree to production in a static format, they should attempt to reach an agreement that the change of the format will have no effect on admissibility. Similarly, if production of some types of ESI is to be in native format, the parties need to agree on a method of use and production that will avoid later claims that the information has been altered.⁹⁴

§ 6.6:2 Keyword Searching vs. Predictive Coding

If a party intends to use keyword or other search techniques to retrieve and collect documents for ultimate discussion, reaching early agreement on those search techniques is essential to avoid later disputes and potential costs of repeated collection efforts.⁹⁵ The court awarded sanctions in *In re Seroquel Products Liability Litigation* partly based on the failure of counsel to work with the opposing party to "reach agreement on appropriate and comprehensive search terms and methods."⁹⁶ In justifying sanctions the court stated, "[i]n this case, AZ never discussed with Plaintiffs which

^{92.} Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007).

^{93.} See Berman, "The Rule 26(f) Conference of the Parties," at 431. Berman urges litigants to: "[c]onsider the problems that may arise in a deposition and at trial if the Rule 26(f) conference results in an agreement that no metadata need be produced and there later arises a genuine question over authenticity of ESI. Or . . . [i]f ESI is converted from native to static format by Rule 26(f) agreement, without any discussion of admissibility, and an authenticity issue is later presented."

^{94.} See chapter 12 of this book for common issues raised as to admissibility of ESI.

^{95.} The Sedona Conference, *The Sedona Conference Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, August 2007 Public Comment Version, 8 Sedona Conf. J. 189, 212 (2007), ("Reaching an early consensus on the scope of searches has the potential to minimize the overall time, cost, and resources spent on such efforts, as well as minimizing the risk of collateral litigation challenging the reasonableness of the search method employed.").

^{96. 244} F.R.D. 650, 662 (M.D. Fla. 2007) (finding the keyword search "plainly inadequate").

search terms to use as part of the search. There was no dialogue to discuss the search terms, as required by Rules 26 and 34."⁹⁷ Areas for discussion include—

- (a) identification of the systems to be searched and those not to be searched;
- (b) restrictions or limitations on the search;
- (c) the use of keyword searches, with an agreement on the words or terms to be searched;
- (d) using sampling to search rather than searching all of the records;
- (e) the number of hours that must be expended by the searching party or person in conducting the search and compiling and reviewing ESI; and
- (f) the amount of preproduction review that is reasonable for the producing party to undertake in light of the considerations set forth in Federal Rule of Civil Procedure 26(b)(2)(C).⁹⁸

Significant advances in predictive coding, or technology-assisted review (TAR), may mean that the parties opt out of key word searching and opt for TAR. Again, this should proceed by agreement. Courts continue to tout the cost-savings of TAR even while acknowledging that the ultimate process of production is in the hands of the responding party.⁹⁹

98. See Suggested Protocol for Discovery of Electronically Stored Information, United States District Court for the District of Maryland (2007). available at http://www.mdd.uscourts.gov/news/news/ esiprotocol.pdf (providing a detailed checklist of requirements for the parties to discuss in the rule 26(f) conference). These factors are adapted from the suggested protocol for conference discussions as to keyword searches. While it is only required in that district, its contents are useful in preparing any e-discovery-intensive case.

^{97.} In re Seroquel, 244 F.R.D. at 664. See clso Romero v. Allstate Insurance Co., 271 F.R.D. 96, 109–10 (E.D. Pa. 2010) (issuing an order compelling "the parties to confer and come to some agreement on the search terms that Defendants intend to use, the custodians they intend to search, the date ranges for their new searches, and any other essential details about the search methodology they intend to implement"); Thomas Y. Allman, Conducting E-Discovery After the Amendments: The Second Wave, 10 Sedona Conf. J. 215, 223 (2009) ("The use of key words has been endorsed as a search method for reducing the need for human review of large volumes of ESI. As noted in the case of In re Seroquel Products Liability, however, it must be 'a cooperative and informed process [which includes] sampling and other quality assurance techniques."").

^{99.} Hyles v. New York City, No. 10 Civ. 3119 (AT)(AJP), 2016 WL 4077114, at *2–3 ("TAR is the best and most efficient search tool. That is perticularly so, according to research studies (cited in Rio Tinto), where the TAR methodology uses continuous active learning ("CAL"), which eliminates issues about the seed set and stabilizing the TAR tool.").

Data Sampling

The rule 26(f) conference is also the appropriate place to initiate conversations about data sampling. "Sampling," as defined by the Sedona Conference, "usually refers to the process of testing a database or a large volume of electronically stored information (ESI) for the existence or frequency of relevant information."¹⁰⁰ Sampling can be a useful tool in a number of ways. It can be used to decide which sources of data will produce fruitful ESI. It can also be used to test the effectiveness of searches or other data extraction procedures. Rule 34(a) now contemplates that a party may seek to "test or sample" electronically stored information.¹⁰¹ But as the advisory committee commented, "[t]he addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances."¹⁰² Direct access requests may enter the picture due to concerns over production or when the discovery compels production of information from databases.¹⁰³ Sampling may also be useful in testing whether keyword searches are capturing material that is at the core of relevant information. Further, Sedona Principle 11 specifically condones the use of data sampling or searching in meeting one's good faith obligation in responding to discovery.¹⁰⁴ Taking this information into account will aptly prepare counsel for the 26(f) meet and confer requirement.

§ 6.6:4 Phased Discovery

Implementing one or more of the proposals outlined above may call for phased discovery. Discovery may be phased according to subject matter in any given case (for example, an initial phase of product identification in products cases, or fact witness testimony in a personal injury case followed by expert discovery). In cases involving the production of voluminous amounts of ESI, the parties may agree to begin discovery with production from the most relevant sources (including key custodians), with-

§ 6.6:3

^{100.} The Sedona Conference, The Sedona Conference Glossary, at 353.

^{101.} Fed. R. Civ. P. 34(a) advisory committee's note (2006) (noting that the amendment is to "make clear that parties may request an opportunity to test or sample materials sought under the rule in addition to inspecting and copying them"); *see also* Allman, *Conducting E-Discovery*, at 225 ("A typical example [of when a party will seek a test or sample] occurs when a requesting party seeks direct access because of its concerns over compliance with discovery obligations.").

^{102.} Fed. R. Civ. P. 34(a) advisory committee's note (2006).

^{103.} See Aguilar, 255 F.R.D. at 364.

^{104.} The Sedona Conference, The Sedona Principles, Principle 11, at 164.

out prejudice to the requesting party to seek more discovery after conclusion of the first stage review.¹⁰⁵ Similarly, if the parties are employing various search techniques, the initial phase of the discovery may be based on preliminary agreed-on searches, with a secondary permissible phase in which the parties may seek information that was expected, but not yielded, by the initial searches.

§ 6.6:5 Expert Discovery

The obligation to preserve and produce applies to some expert witness material, but other material is work-product protected.¹⁰⁶ To preempt later disputes, counsel should confer early about what categories of material should be produced, what may be withheld, and, even better, what does or does not need to be identified on a privilege log.

§ 6.7 Preparing for the Conference

"Cooperation . . . requires . . . that counsel adequately prepare prior to conferring with opposing counsel to identify custodians and likely sources of relevant ESI, and the steps and costs required to access that information. It requires disclosure and dialogue on the parameters of preservation."¹⁰⁷ As this chapter suggests, planning for the rule 26(f) conference should not be a "fly by night" attempt to wing it and then stall on discovery. Preparation begins with understanding the requirements of discovery under the federal rules and the potential sources of ESI available. Reading this book is a good start. Before embarking on any case involving ESI, counsel should also read Federal Rules of Civil Procedure 16, 26, 34, and 37, and the 2006 advisory committee comments explaining the changes to these rules that specifically address ESI.¹⁰⁸

Counsel should also research whether the local rules or the presiding judge's rules require coverage of specific topics in the rule 26(f) conference, or a report in a spe-

^{105.} See Moore v. Publicis Groupe, 287 F.R.D. 182, 193 (S.D.N.Y. 2012), adopted sub nom. Moore v. Publicis Groupe SA, No. 11 Civ. 1279(ALC)(AJP), 2012 WL 1446534 (S.D.N.Y. Apr. 26, 2012).

^{106.} Fed. R. Civ. P. 26(b)(4).

^{107.} The Sedona Conference, *The Case for Cooperation*, 10 Sedona Conf. J. 339, 344 (2009) (emphasis in original).

^{108.} Rules 33 and 45 were also amended in 2006 and should also be read in preparation for any ESI case. Additional recommended reading includes: The Sedona Conference, *The Sedona Principles*; The Sedona Conference, *Working Group One on Electronic Document Retention and Production* (2009); and The Sedona Conference Working Group Series, *The Sedona Conference Cooperation Proclamation*, 10 Sedona Conf. J. 331 (2009). These materials are also recommended for judges presiding over litigation involving e-discovery. *See* The Sedona Conference, *The Sedona Conference Cooperation Proclamation: Resources for the Judiciary*, at 9 (2014), *available at* https://thesedonaconference.org/publication/ Resources_for_the_Judiciary.

cific form.¹⁰⁹ At least one federal district judge in Texas has drafted specific guidelines for attorneys to use in conducting their rule 26(f) conference.¹¹⁰

The next step should be strategically thinking about the case themes, goals of discovery, and litigation plan. Some important questions to consider:

- What are the elements of the cause of action pleaded?
- What information will you need to prove your client's case and how will you get it from your client, opposing parties, or potential third parties?¹¹¹
- Where is that information likely to reside and who are the key custodians likely to have it?
- What types of data are at issue? For example, are communications via email, text message, or voice message at issue?
- Is information contained in structured databases?
- Are some sources more likely to include relevant information than others?¹¹²

Developing a factual timeline from the outset can be invaluable.

The next step should be familiarizing yourself with your clients' own information systems and document retention policy.¹¹³ The Sedona Conference has published "Jump-Start Outline": Questions to Ask Your Client & Your Adversary to Prepare for Preservation, Rule 26 Obligations, Court Conferences & Requests for Production,¹¹⁴

112. See The Sedona Conference Working Group Series, The Sedona Conference: Cooperation Guidance for Litigators & In-House Counsel, at 3 (2011), available at https:

//thesedonaconference.org/sites/default/files/publications/Cooperation_Guidance_for_Litigators _and_In_House_Counsel.pdf. ("It is important to note that these early conversations will set the tone for the case and counsel should approach each other with professionalism.").

113. See Fed. R. Civ. P. 26(f) advisory committee's note (2006) ("It may be important for the parties to discuss those [information] systems and accordingly important for counsel to become familiar with those systems before the conference.").

^{109.} See The Sedona Conference, The Sedona Conference Cooperation Proclamation: Resources for the Judiciary.

^{110.} See The Honorable Xavier Rodriguez, Scheduling and Docket Control Order, available at http://www.txwd.uscourts.gov/Rules/StandingOrders/SanAntonio/sched_xr.pdf.

^{111.} In *Rodriguez-Torres v. Government Development Bank of Puerto Rico*, 708 F. Supp. 2d 195, 199 (D.P.R. 2010), the court awarded attorney's fees to the defendants for having to respond to plaintiff's motions regarding preservation, the litigation hold, and to compel discovery, in part because the plaintiffs had "the opportunity to request electronic discovery" at the rule 26(f) conference and the initial scheduling conference, "but failed to do so."

which is a good checklist of items to cover in preparing for a rule 26(f) conference. The list urges counsel to seek information on the following items:

- The client's information systems structure.
- Is there a network-based system? What is the configuration?
- Are there any databases at issue with active information that may need to be preserved?
- How much of the ESI is duplicative of ESI that will be collected?
- How dispersed is relevant ESI with nonrelevant information?
- The client's document retention policy, and whether it should be suspended.
- Preservation efforts to date, including the issuance and scope of a litigation hold.
- The need to preserve (or take a snapshot) of any active databases that may change over time.
- The need to preserve any archived or legacy data, including backup tapes. (As a corollary, one should also seek information on the expense and burden of restoring such legacy data should it be requested.)
- The locations and custodians of data, communications, or other ESI.
- The time parameters for relevant ESI: Should litigation hold documents cover future information? Should document collection efforts be ongoing? Is there a cutoff in time for which there is not likely to be any relevant ESI after a date certain?
- The use of external media by clients and employees and preservation of that media.
- The likelihood of relevant ESI on the employees' or the client's home computers, smartphones, tablets, or other devices, and reasonable steps that may be taken to preserve and collect such information.
- The likelihood that relevant ESI is held by third parties.¹¹⁵

^{114.} Ariana J. Tadler, Kevin F. Brady, Kerin Scholz Jenson, *The Sedona Conference "JumpStart Outline": Questions to Ask Your Client & Your Adversary to Prepare for Preservation, Rule 26 Obligations, Court Conferences & Requests for Production* (March 2016), *available at* https://thesedonaconference.org/publication/Jumpstart Outline.

^{115.} Tadler et al., The Sedona Conference "JumpStart Outline."

The primary goal is to educate oneself about how and with whom potentially relevant ESI is stored. This will involve interviewing your client about their practices: How is e-mail created? How is it retained? How are business documents created and retained? How is research conducted? Who are the key players who may have relevant information? With respect to backups, you will want to know how often backups are created and recycled pursuant to the normal document retention policy. To the extent backup tapes exist, what is the cost and method of restoration?¹¹⁶ Keep in mind that rule 26(b)(2)(B) does not require the production of information "from sources that the party identifies as not reasonably accessible because of undue burden or costs."117 If you or your client claim some source of ESI is not reasonably accessible, what information will you provide opposing counsel and the court to justify this assessment? In conducting this investigation, you should discuss with your client the scope of production the client is willing to undertake, the ultimate form of production preferred, and whether there is any ESI that is not reasonably available. You will also need to consider whether the ESI implicates privacy concerns or proprietary business information necessitating a protective order.

Another consideration is whether your client has a suitable e-discovery representative who can assist you in preparing for the rule 26(f) conference and even attend the conference to provide substantive input. You may request that the opposing party similarly bring a representative of the client fully informed in their information systems. In large to medium-sized cases, it is recommended to meet in person with the client and key custodians before the rule 26(f) conference to discuss your own checklist of requests and visit with any information systems personnel and key factual players in person.¹¹⁸

^{116.} Tadler et al., The Sedona Conference "JumpStart Outline."

^{117.} See Fed. R. Civ. P. 26(b)(2)(B) (stating that although one might decide through consulting with a client that information is not reasonably accessible, it may still be advisable to preserve such information in the event a court does not agree with this assessment).

^{118.} I have done this in cases with a willing client, and it has proved invaluable. In other cases in which the client was less willing to engage in extensive research at the outset of the case, it invariably led to discovery issues due to lack of adequate information. *See* Moze Cowper & John Rosenthal, *Not Your Mother's Rule 26(f) Conference Anymore*, 8 Sedona Conf. J. 261, 263 (2007) (advocating a preconference in-person meeting with the client). The question becomes, of course, whether such cost is justified. *See* Steven S. Gensler, *Some Thoughts on the Lawyer's E-Volving Duties in Discovery*, 36 N. Ky. L. Rev. 521, 536–37 (2009) (discussing the various issues with costs and e-discovery noting that one such issue is "changes in when and how costs are incurred [that] can alter the dynamics of settlement"); *see also* The Sedona Conference. *Cooperation Guidance*, at 22 ("Before the Rule 26(f) Meet and Confer, in-house counsel should take the lead in coordinating meetings between outside counsel, business units responsible for the responsive ESI, and appropriate IT department personnel that provide underlying administration support for the data.").

Much like preparing for a deposition, you should consider the tone with which you would like the conference to proceed. The goal embraced by the federal rules and the Sedona Conference guidance materials is to proceed with a cooperative spirit. Setting this tone early in the conference is important.¹¹⁹ To make the conference more efficient, the attorneys should consider sending a pre-conference proposal for an agenda and a letter outlining your client's information systems structure, sources of potentially relevant ESI, key custodians discovered to date, and proposals for each of the components of the discovery plan discussed above. Given the needs of any particular case it may make sense to involve third-party technical advisors, mediators, or a special master to facilitate the understanding between the parties of sources of information and search methodologies.¹²⁰ Finally, it is important to recognize that given the iterative process of discovery, particularly when dealing with ESI, the meet and confer requirement is a process. It may require several meetings or telephone calls over time or as new hurdles present themselves. Encouraging cooperation and negotiation from the outset of the case can set the stage for a more fruitful process.

§ 6.8 Cooperation

"The most straightforward reason for parties to cooperate throughout the discovery process is simple economics—unnecessarily combative discovery wastes time and money."¹²¹ Rule 26 imposes an obligation of "good faith" in attempting to agree on the proposed discovery plan, but beyond this obligation does not clarify the degree to which cooperation is required.¹²² As noted above, setting the cooperative tone and decisions about the degree of disclosure the client is willing to make are strategies that should be discussed before the rule 26(f) conference takes place.¹²³ The Sedona Conference has published *The Cooperation Proclamation*, which calls for a "paradigm shift" to "promote pre-trial discovery cooperation."¹²⁴ The Proclamation "promote[s] open and forthright information sharing, dialogue (internal and external), training, and

^{119.} See The Sedona Conference, *The Sedona Conference: Cooperation Guidance*, at 3 ("It is important to note that these early conversations will set the tone for the case and counsel should approach each other with professionalism.").

^{120.} See The Sedona Conference, *The Sedona Conference: Cooperation Guidance*, at 5–6 (recognizing that "technical expertise asymmetry" coulc impede meaningful agreement, and encouraging the use of third parties with expertise to "provide both sides comfort and practical solutions").

^{121.} The Sedona Conference, "The Case for Cooperation," at 356 (discussing the economic incentives to cooperation in ESI discovery).

^{122.} Fed. R. Civ. P. 26(f).

^{123.} Fed. R. Civ. P. 26(f) advisory committee's note (2006).

^{124.} The Sedona Conference, *The Sedona Conference Cooperation Proclamation*, 10 Sedona Conf. J. 331, 333 (2009).

the development of practical tools to facilitate cooperative, collaborative, transparent discovery."¹²⁵ Not surprisingly, a number of federal and state judges have endorsed *The Cooperation Proclamation*, including twelve Texas judges as of July 2019.¹²⁶

Since its publication, many courts have invoked the principles of *The Cooperation Proclamation* in deciding discovery disputes.¹²⁷ The authors of the conference posit the well-founded argument that cooperation is required by the Federal Rules of Civil Procedure,¹²⁸ and by ethical rules, including the duties to expedite litigation, provide competent representation, and the duty of candor to the tribunal and fairness to the opposing party.¹²⁹ But beyond what legal and ethical rules require, there is a second level of cooperation promoted by the spirit of the e-discovery amendments to the federal rules and by the economics of e-discovery. Under this second level of cooperation, as envisioned by the authors of the Proclamation:

126. See The Sedona Conference Working Group Series, "Judicial Endorsements" in The Sedona Conference Cooperation Proclamation (2019), available at https://thesedonaconference.org/sites/ default/files/publications/judicial endorsements 0.pdf.

127. See, e.g., Cornell Pump Co. v. Thompson Pump Manufacturing Co., No. 6:17-cv-847-Orl-41TBS, 2018 WL 3827248, at *3 (M.D. Fla. Feb. 22, 2018) (declining to resolve discovery dispute in hopes parties will proceed cooperatively and noting "the parties are advised that the undersigned subscribes to the views expressed in The Sedona Conference Cooperation Proclamation."); Hyles v. New York City, No. 10 Civ. 3119 (AT)(AJP), 2016 WL 4077114, at *2-3 (S.D.N.Y Aug. 1, 2016) (refusing to force responding party to use predictive coding even while touting its advantages when the responding party preferred a keyword search, based on The Sedona Principles and The Cooperation Proclamation); Kleen Products LLC v. Packaging Corp. of America, No. 10 C 5711, 2012 WL 4498465, at *19 (N.D. Ill. Sept. 28, 2012), objections overruled, 2013 WL 120240 (N.D. Ill. Jan. 9, 2013) (following principles outlined in The Cooperation Proclamation and noting that collaborative "approach should be started early in the case [because it] is difficult or impossible to unwind procedures that have already been implemented."); Tadayon v. Greyhound Lines, Inc., No. 10-1326 (ABJ/JMF), 2012 WL 2048257, at *6 (D.D.C. June 6, 2012) (declaring that "there is a new sheriff in town" and ordering "the parties, without surrendering any of their rights, [to] make genuine efforts to engage in the cooperative discovery regimen contemplated by the Sedona Conference Cooperation Proclamation."); Cartel Asset Management v. Ocwen Financial Corp., No. 01-cv-01644-REB-CBS, 2010 WL 502721, at *13-14 (D. Colo. Feb. 8, 2010) (putting counsel on notice that "this court will expect them to confer in good faith and make reasonable efforts to work together consistent with well-established case law and the principles underlying The Cooperation Proclamation").

128. The Sedona Conference, *The Sedona Conference: Cooperation Proclamation*, at 332 (finding the 2006 amendments to the Federal Rules of Civil Procedure to emphasize early communication and cooperation and observing that discovery rules frequently compel parties to meet and confer with other parties, and to certify that they have attempted in good faith to resolve discovery disputes).

129. The Sedona Conference, The Case for Cooperation, at 339-41.

^{125.} The Sedona Conference, *The Sedona Conference: Cooperation Proclamation*, at 331. To this end, *The Sedona Conference*, as Part III of the Cooperation Proclamation, develops "toolkits" to support lawyers, judges, students, and other professionals in the techniques of cooperation. The Sedona Conference: *Cooperation Proclamation*, at 333.

[T]he parties work together to develop, test and agree on the nature of information being sought. They will jointly explore the best method of solving discovery problems, especially those involving [ESI]. The parties jointly address questions of burden and proportionality, seeking to narrow discovery requests and preservation requirements as much as reasonable.¹³⁰

The Cooperation Proclamation recognizes the following methods to act cooperatively.

- 1. Utilizing internal ESI discovery "point persons" to assist counsel in preparing requests and responses.
- 2. Exchanging information on relevant data sources, including those not being searched, or scheduling early disclosures on the topic of electronically stored information.
- 3. Jointly developing automated search and retrieval methodologies to cull relevant information.
- 4. Promoting early identification of form or forms of production.
- 5. Developing case-long discovery budgets based on proportionality principles.
- 6. Considering court-appointed experts, volunteer mediators, or formal ADR programs to resolve discovery disputes.¹³¹

What can be garnered from these explanations is that cooperation is not a one-size-fits-all metric. It must be tailored to the size, complexity, and players in the case. But at its essence, it involves a mutually beneficial exchange of information that does not undermine the substantive positions of the parties and that preserves the assertion of privilege over such material.¹³²

132. The formulation for this definition was provided by David Kessler, cohead of e-discovery and information practice at Fulbright & Jaworski, LLP. Thanks to David for his thoughts in this area.

^{130.} The Sedona Conference, *The Case for Cooperation*, at 339. Cooperation is perhaps more easily defined by what it is not. In one interesting Texas case, the Texas attorney general sought a declaratory judgment that the plaintiff's pre-suit litigation hold violated the recently revised rules 26 and 34 as to the electronic discovery requests. *Texas v. City of Frisco*, No. 4:07cv383, 2008 WL 828055, at *3 (E.D. Tex. Mar. 27, 2008). The court dismissed the suit as nonjusticiable because it was not ripe, but went on to note, "[f]urther, while they do not specifically address pre-suit litigation hold requests, the Rules of Civil Procedure contemplate that the parties will act in good faith in the preservation and production of documents. *See* Fed. R. Civ. P. 37. The Court encourages both parties to handle the preservation of documents in response to their respective litigation holds in such good faith." *City of Frisco*, 2008 WL 828055, at *4.

^{131.} The Sedona Conference, The Sedona Conference: Cooperation Proclamation, at 332.

The duty to cooperate is not simply a lofty ideal with no "teeth." Courts have awarded and will continue to award sanctions for failure to engage in the iterative "give and take" process rule 26(f) envisions. In *Mancia v. Mayflower Textile Services Co.*, Judge Grimm invoked rule 26(g) as charging "those responsible for the success or failure of pretrial discovery—the trial judge and the lawyers for the adverse parties—with approaching the process properly."¹³³ If the parties fail to do so, "the judge is expected to impose appropriate sanctions to punish and deter."¹³⁴ Referred to by Judge Grimm as "one of the most important, but apparently least understood or followed" discovery rules, rule 26(g) requires, at its most basic, that every disclosure, every discovery request, response, or objection "must be signed by at least one attorney of record."¹³⁵ The signature is the certification of the attorney "that to the *best of the person's knowledge, information, and belief formed after a reasonable inquiry*":¹³⁶

- (A) with respect to a disclosure, it is complete and correct as of the time it is made; and
- (B) with respect to a discovery request, response, or objection, it is:
 - (i) consistent with these rules and warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law, or for establishing new law;
 - (ii) not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and
 - (iii) neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action.¹³⁷

According to the advisory committee's note to rule 26(g), it "imposes an affirmative duty to engage in pretrial discovery in a responsible manner that is consistent with the spirit and purposes of Rules 26 through 37."¹³⁸ Rule 26(g) curbs discovery abuse by "explicitly encouraging the imposition of sanctions," which should serve as a deter-

^{133. 253} F.R.D. 354, 360 (D. Md. 2008).

^{134.} Mancia, 253 F.R.D. at 356.

^{135.} Mancia, 253 F.R.D. at 357. See also Fed. R. Civ. P. 26(g).

^{136.} Mancia, 253 F.R.D. at 357 (emphasis added).

^{137.} Fed. R. Civ. P. 26(g)(1).

^{138.} Fed. R. Civ. P. 26(g) advisory committee's note (2006).

rent to excessive discovery and evasion. Similarly, in *Romero v. Allstate Insurance Co.*, the court ordered the parties to meet and confer "in a cooperative, rather than adversarial, manner to resolve discovery issues."¹³⁹ Among the issues the court expected agreement on were search terms, custodians, and date ranges for the search methodology.

The question posed by attorneys resisting the cooperative approach is how does one pursue zealous advocacy of one's client by giving information to the other side? But this rests on the misfounded idea that adversarial conduct equals advocacy. As the drafters of the Proclamation recognize: "[c]ooperation does not conflict with the advancement of their clients' interests—it enhances it. Only when lawyers confuse advocacy with adversarial conduct are these twin duties in conflict."¹⁴⁰ Judge Peck addressed the standard well in *Moore v. Publicis Groupe*:

Another way to phrase cooperation is "strategic proactive disclosure of information," i.e., if you are knowledgeable about and tell the other side who your key custodians are and how you propose to search for the requested documents, opposing counsel and the Court are more apt to agree to your approach.¹⁴¹

§ 6.9 Conclusion

The rule 26(f) conference has traditionally been seen as just another procedural hurdle to cross before case preparation can begin. The increasingly complex and simultaneous "everyday" nature of ESI and the 2006 amendments to rule 26 should change that perception. The rule 26(f) conference is an excellent opportunity to cut discovery costs, reach real agreements with opposing counsel that can speed discovery, and result in fewer "document dumps" and less expensive review processes. The 2006 amendments support innovative strategies such as keyword searches, data sampling, and quick-peek agreements all with an eye toward alleviating the massive e-discovery costs that are crippling access to the courts. A fully prepared counsel with a healthy eye toward cooperation can do much to avoid discovery pitfalls down the road, and at the very least proceed through discovery with significant parameters in place.

^{139. 271} F.R.D. 96, 109–110 (E.D. Pa. 2010) (citing The Sedona Conference, The Case for Cooperation, at 344–45).

^{140.} The Sedona Conference, *The Sedona Conference: Cooperation Proclamation*, at 331. *See also Cartel Asset Management*, 2010 WL 502721 at *13–14 (recognizing that cooperative conduct in discovery conferral does not conflict with the advocacy of the client's interests).

^{141. 287} F.R.D. at 193.



Chapter 7

ESI Collection

Emma Cano

§ 7.1 Introduction

ESI collection can involve a considerable undertaking by parties responding to discovery requests. But, with adequate planning and preparation, practitioners can streamline the process and prepare for production of ESI in an efficient and comprehensive manner. While the time this process can take largely depends on the volume of data, the size of the organization, and its technological capabilities and practices, practitioners are well-advised to begin their ESI collection efforts early on in the litigation. They should assess the universe of electronic data as early as possible to enable them to plan their efforts accordingly and to determine whether ESI will be produced through discovery. Waiting until a request for ESI is received may leave the responding party without enough time to adequately identify, review, and produce electronic data and may cause unnecessary frustrations. Depending on the volume of existing data, the standard thirty-day period for responding to discovery may be insufficient. Thus, responding parties should begin their ESI collection efforts as soon as reasonably practicable.

Practice Tip: If possible, do not wait until you have received discovery requests to begin collecting ESI. That being said, costs may also be a significant consideration affecting the decision of when to begin these efforts.

The subject of ESI collection can be generally divided into two steps, both of which will be addressed separately in this chapter. First, the responding party must identify responsive ESI. Then, it must actually collect the data. Each step is equally important, and if not done carefully and comprehensively, the responding party can effectively frustrate the discovery process.

§ 7.2 Identifying Relevant ESI

The first step of a party's ESI collection efforts entails a thorough investigation of the client's practices and technology operations to identify existing ESI. This investigation requires practitioners to delve into the client's customs, routines, and policies to

identify the universe of potentially relevant data. The best way to do this is to consult with the client's IT department, if they have one, or to interview the individuals who handle the client's technology operations. The key is to identify the individuals who best know the relevant technology structure and can assist the attorney to conduct a thorough investigation. Once the attorney has a good understanding of the organization's technology structure and routine, he must then inquire about the relevant custodians' particular technology habits and practices, ideally through direct custodian interviews. Practitioners must have a good grasp of the existing data before actually beginning collection efforts. Therefore, this section discusses various topics that practitioners should explore and strive to understand to maximize their collection efforts.

§ 7.2:1 Conducting IT Interviews

When interviewing an organization's IT or technology representative(s), attorneys should try to get as thorough a picture of the organization's electronic structure to ensure that the search for all potentially responsive data includes all likely locations where data might reside.¹ In its most basic form, you should understand what type of technology system the organization has, and how and where the organization stores its electronic data. Obviously, the organization's size and the sophistication of its technology operations will dictate the complexity of this part of the investigation. Regardless, attorneys must ask many questions and conduct as detailed an inquiry as possible.

§ 7.2:2 Document/Record Retention Policies

When conducting IT or technology representative interviews, one of the first questions practitioners must ask is whether a document or record retention policy exists, because its existence, or lack thereof, can have different implications for the responding party. A document retention policy is a systematic plan for reviewing, maintaining, and destroying documents and data, including hard-copy and electronic documents, databases, and e-mails, that are created, sent, and received in an organization's ordinary course of business.² See Chapter 3—Computer Usage Policies, Records Management and Information Governance.

^{1.} See Table 7-1 for a guide that can assist you in conducting IT or technology representative interviews.

^{2.} See www.edrm.net/glossary/document-retention-policy/.

A document retention policy, which allows for the routine and periodic destruction of data after a prescribed period of time, can protect your client from allegations of spoliation (i.e., the negligent or intentional destruction of data). If the organization routinely discards old data in accordance with its document retention policy, it is unlikely that the requesting party can establish that the party breached any duty to preserve. Obviously, the resulting protection afforded by complying with a company's document retention policy does not excuse the destruction of data when the party knows or should know that it possesses evidence relevant to potential or ongoing litigation.³ The existence of the duty to preserve and the use of evidence preservation letters or litigations holds are discussed in Chapter 1—Duty to Preserve and Chapter 2—Litigation Holds, respectively.

The existence of a document retention policy and an organization's strict adherence to that policy can significantly minimize the amount of potentially responsive data that must be analyzed. For example, if the company's document retention policy mandates the destruction of e-mail older than six months and the company follows its policy, you may find very few e-mail exchanges pertaining to a contract negotiation that occurred four years earlier. However, if the organization lacks a document retention policy, the relevant e-mail data likely still exists somewhere, and your client may be forced to go back a significant length of time to collect the requested data.

§ 7.2:3 Former Employees

Because employees come and go, attorneys must inquire about the organization's procedures for handling departing employees. What happens to an employee's electronic data when that individual's employment status changes—is the individual's e-mail and other electronic data somehow preserved (whether by saving the computer or hard drive, or extracting and preserving the data), or is the computer wiped upon departure? What happens to the individual's hard-copy files—are they preserved or discarded? If the electronic data or hard-copy files are saved or preserved in some manner, the responding party has an obligation to produce it in response to applicable requests for production.

^{3.} See Wal-Mart Stores v. Johnson, 106 S.W.3d 718, 722 (Tex. 2003) (stating that party must preserve evidence that is relevant to potential or ongoing litigation); *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 73 (S.D.N.Y. 1991) (noting that duty to preserve evidence begins with counsel, "who [has] a duty to advise his client of the type of information potentially relevant to the lawsuit and of the necessity of preventing its destruction").

§ 7.2:4 File Servers

Practitioners should understand the organization's file servers because that is where most of the electronic data will be stored. File servers are designed to allow for the storage and retrieval of data by multiple computers or workstations on a shared network. If the organization only has one server, the inquiry ends there. However, if multiple servers are used by the organization, then you have to identify which servers might contain potentially relevant data. When the organization utilizes multiple servers, a data map might allow the producing party to minimize the number of unnecessary searches for data by generally identifying the content of those servers.

Practice Tip: Obtain or create a data map tracking the organization's servers and the data assigned to each particular server.

How many servers does the organization utilize? Oftentimes, particular servers are assigned to certain departments or employees. Thus, if you need to produce e-mails generated or received by one individual, you might be able to limit your inquiry to the particular server that services that employee rather than having to search all the organization's servers. Practitioners should understand whether there are multiple office locations and how the servers are allocated with respect to those offices to determine which servers need to be accessed in search of potentially relevant electronic data. What type of servers does the organization utilize? Do they have dedicated servers for e-mail, shared drives, user home drives, accounting, or other systems within the organization? Does the organization use third-party service providers to store its electronic data? All of these questions are designed to identify particular locations of potentially relevant ESI.

§ 7.2:5 System Details

Practitioners should also seek to understand details about the organization's technology systems. What kind of computers or equipment do individuals utilize? Do they have desktops, laptops, or a combination of the two? Do they have smartphones or other PDA-like equipment? What type and version of operating system does the organization use? What type of e-mail system is used? Do they have a shared network, and what information is stored on that network? Do they utilize webmail? Do individuals have POP3 e-mail accounts, such as Gmail, Hotmail, Yahoo, or other such accounts? A thorough investigation that includes these type of questions will help ensure the responding party searches all potential data storage locations. In the ever-changing digital world, almost everyone uses mobile phones. Many of those mobile phones have smart technology capable of retaining, accessing, and utilizing more data than ever before. Because these technological advancements are so prevalent in our everyday lives, any ESI collection efforts must specifically consider mobile phones and whether they might contain relevant data that needs to be collected. This includes e-mail stored on mobile phones, text messages, instant messaging applications, etc. Such assessments should consider whether such data has been otherwise collected or whether it is unique data that needs to be retrieved. For example, people often access e-mail on their mobile phones as well as their computers. In such instances, you only need to collect the data once to avoid unnecessary and extra work. Thus, if the specific e-mail account has already been collected from the server or directly from the computer, there is no need to also collect that e-mail from the mobile phone.

Text messages and instant messaging conversations can be a little trickier because of the way that data is received and the format in which it is stored on the phone. Thankfully, there are specific tools and applications designed to ensure the collected data includes the substantive message, as well as identifying information about the phone numbers involved in the messages, the time and date of the message, etc. This data can be very helpful when trying to utilize such communications, and is crucial to any effort to make such communications admissible in court.

Practice Tip: Identify all mobile phones that could contain potentially relevant data and information. If an e-mail account has otherwise been collected, do not duplicate these efforts by also collecting from the mobile phone.

Use specialized tools or applications to help collect text messages and instant messaging conversations, or consult with a professional who can help ensure these messages are properly collected.

§ 7.2:7 Miscellaneous Considerations

When trying to identify all possible locations where electronic data might reside, practitioners are advised to consider a few additional matters so as to adequately assess existing data and determine its relevance. Does the organization or relevant individual(s) participate on one of the many available and commonly used social networks? If so, there could be potentially relevant data stored on external sites or networks not controlled by the responding organization. Does the organization utilize

instant messaging? If so, these communications would not be found in the various custodian e-mail files. Instead, separate instant message logs that record those communications likely exist and must be separately obtained. Are voice mails received by individuals within an organization automatically converted to WAV files? If so, the responsive data might look a little different than a standard e-mail file. Is the organization required to save email for a prescribed time period? For example, energy traders or other regulated industries are required to save e-mail for a certain period of time during which it cannot be discarded. If so, data might be stored longer than usual and responding parties must adequately search for the potentially responsive data.

Could connected home devices have relevant data or evidence? There are circumstances when this could happen, so consider any home devices such as Amazon's Alexa, Google Home, or Apple HomePod, and determine whether to collect information from those devices' storage locations. Instances of such information being sought have already started surfacing in criminal prosecution cases, and it certainly is conceivable that such information could be sought in civil cases as well.

What about personal wearable technology, such as Fitbit or Garmin devices? Such devices might contain relevant information or data that should be considered. While it is unlikely that such devices will lead to the discovery of relevant electronic data in every instance, there are some circumstances in which such data might be relevant. In January 2019, a British man was convicted for the murder of two gangsters because of data recovered from his GPS watch.⁴ Although police already suspected the runner, cyclist, and mob hitman for the murders, GPS data from the man's Garmin Forerunner device linked him to the location of the murder and confirmed that he had visited his target's neighborhood in the short time before the murder occurred. Again, while unlikely to be relevant in every instance, one should at least consider the existence of such wearable devices and whether such data might be useful and/or relevant.

§ 7.3 Conducting Individual Custodian Interviews

Once the practitioner has a good understanding of the organization's overall technology systems and structure, he must then investigate the specific custodians that are likely to possess the relevant data and their individual habits and practices.⁵ While the organization's technology structure is certainly important, the custodians are the individuals who actually work with the data—creating, receiving, storing, and deleting it.

^{4.} See www.runnersworld.com/news/a25924256/mark-fellows-runner-hitman -murder/.

^{5.} See Table 7-2 for a guide that can assist you in conducting individual custodian interviews.

The goal is to be as thorough as possible so that relevant responsive data is captured for eventual production. Therefore, practitioners should have detailed and thorough conversations with relevant custodians to ensure that relevant electronic data is identified, and to the extent necessary, eventually collected.

§ 7.3:1 Individual Workstations

When interviewing custodians, practitioners should first gather information about the individual's workstation and setup. Does the employee use a PC or Apple computer? Is it a desktop, laptop, or both? What is the make/model of the computer? What operating system does the workstation use? What is the size of the hard drive? These basic details about the computer setup are good background information that might be useful in the impending collection efforts.

The distinction between PC and Apple computers is extremely relevant to collecting and processing ESI and is one that merits further discussion.⁶ Over the past decade, there has been a significant increase in usage of Apple computers and devices by corporate America. However, most ESI collection and review software was not initially designed for Apple devices and collection efforts often result in generating "unsupported" files, although tools and applications continue to evolve and have drastically improved to better support collections from Apple devices. Thus, a party's ESI collection (and subsequently, production) could result in a party failing to produce certain responsive data in a reasonably usable and accessible form. However, despite being "unsupported," ESI from Apple devices is still discoverable, and parties are still obligated to produce responsive, discoverable data. Thus, parties should take calculated steps to ensure that their collection and review efforts fully address any issues involving Apple devices and ESI. For example, certain collection tools can help process and convert Apple ESI so that it can be adequately collected. Likewise, certain data processing services address these issues in a manner that still protects the structural integrity of the ESI's metadata. When Apple ESI is involved or potentially involved in a production, be sure to discuss with your e-discovery service provider their ability to handle Apple ESI before committing to utilizing their services. Failing to adequately address these issues can result in deficient collections and productions that fail to comply with applicable rules of discovery.

^{6.} For a detailed discussion of this issue, see Joshua Gilliland, *Exotic Apples: Solutions In Collecting & Processing Apple ESI*, Bow Tie Law's Blog (August 15, 2011), at http://bowtielaw.wordpress.com/2011/08/15/exotic-apples-solutions-in-collecting-processing-apple-esi/.

Practice Tip: When Apple devices are involved, always take adequate precautions to ensure that the data is properly collected and processed so that it can be reviewed.

§ 7.3:2 Software

Custodian interviews should also include discussions about the type of software regularly used by the individual. What software is used on a daily basis? For example, Lotus Notes, Word, Excel, etc. Additionally, it is important to identify whether specialty software (e.g., AutoCAD, Photoshop, QuickBooks) is routinely used. Certain precautions will have to be taken to ensure that specialty software files can actually be viewed through the selected review platform. Sometimes the specialty software might have to be obtained so that the files can be adequately viewed. Otherwise a workaround must be created. It is important to discuss your vendor's capabilities with respect to specialty software that might be involved with your production.

§ 7.3:3 Network Information

Discussions with custodians should also address whether the individual is connected to a network. If so, you must ascertain the location (i.e., the city or particular office) of the server because that is where the data resides, and the relevant server(s) must be included in any ESI collection efforts.

§ 7.3:4 Relevant Data

Collection efforts should extend to all individuals who possess relevant and responsive data. Practitioners should therefore specifically address the existence of relevant data with the identified custodians during the course of the ESI investigation. If the custodian possesses relevant data, practitioners should understand the format of that relevant data. For example, if it involves e-mail files, are they PST, OST, or MSG files? If the individual is in the accounting department, are they QuickBooks files or Excel files? If the individual maintains hard-copy data, where are the files stored or maintained? All of these questions are crucial to your precollection efforts.

§ 7.3:5 Data Storage and Backup

Finally, practitioners should thoroughly understand the custodian's data storage and backup routine, habits, and practices because these will dictate where to look for relevant ESI. Having a good understanding of where the individual actually saves data will help target the collection efforts and could help limit unnecessary searches of locations that aren't likely to house the data being sought. Is data saved locally on the computer? Is it saved on a shared network? Is it saved on a home directory? Does the individual use thumb drives or other external drives? Does the individual save data on a smartphone or PDA-like device? Does the individual use cloud storage? What document management system does the individual use? All of these questions will help identify potential locations of ESI. Additionally, practitioners will want to identify all databases that may contain responsive data and ascertain the path/folder name for relevant data in preparation for collection. Understanding the individual's backup routine could also help practitioners identify the existence of relevant ESI. If the individual backs up his computer locally, what type of media and software does he use for these efforts? Furthermore, how long is the backup data preserved? This information can help the practitioner properly assess and identify the universe of relevant ESI possessed by the client.

§ 7.4 Collecting ESI

Once practitioners have a good and detailed understanding of their client's ESI, its format, its location, and any particularities about the data, the next step involves actually collecting the data. While this can be done in a number of ways, the key to data collection is to ensure that individual(s) actually doing the collection understand the goal (i.e., to capture and collect as much targeted data and ESI as exists) and are proficient with the technology being utilized for the collection. Federal Rule of Evidence 902 was amended in 2017 to allow for authenticity of electronic evidence to be established without having to incur the burden and expense of producing an authentication witness if the person retrieving the data was qualified to do so and provides the requisite certification. Fed. R. Evid. 902(13) and 902(14). Thus, there is a certain competence inherently required in any efforts to collect the data, at least for purposes of authenticity. (Such certification does not affect other objections.)

This section addresses various collection methods, provides pointers, and identifies some dangers associated with ESI collections.

Practice Tip: All individuals involved in collecting ESI should possess a toolkit consisting of at least the following:

1. FTP server;⁷

^{7.} An FTP (file transfer protocol) server allows for the exchange of files over the Internet. This can be used to obtain data from clients or exchange data with opposing counsel.

- 2. software for copying client files;
- 3. software for processing ESI;
- 4. early case assessment culling tools; and
- 5. review software if not using a hosted solution (i.e., solution offered by a service provider).

§ 7.4:1 Collection Methods

There are several methods that can be used to collect ESI. While there is no right way of doing it, practitioners must ensure that the collection is being done properly, thoroughly, and by someone who understands the process and the intricacies associated with collecting electronic data. Various factors, including the nature of the case, the industry involved, the organization's technology structure, and proportionality, will all affect the decision of which collection method to utilize. Practitioners want to be thorough without being over-inclusive because this can lead to unnecessary expense. Thus, proficiency is key.

Collecting ESI can involve either full replication of the data or targeted collections. The decision of which method to employ should be made prior to beginning the collection to eliminate any unnecessary steps and avoid redundancy. The full replication method involves making a forensic copy of the identified datasets. Full data duplication may only be necessary in limited instances.⁸ However, if this is the desired method, the practitioner is advised to consult with a forensic technician who has the required expertise. Rather than imaging all the data, a targeted collection involves limiting the size and scope of the collection to certain parameters that meet the intended collection, such as by limiting the custodians, limiting file types, or conducting keyword searches. Once the decision is made whether to conduct a full replication or a targeted collection, there are several options available to actually conduct the collection.

^{8. &}quot;[F]orensic collections like this typically are necessary only in cases involving computer-based fraud, IP theft, or when user-specific computer habits are at issue." James Bernard, Michael Quartararo, Jason Vinokur, E-discovery: What to do (and not do) when collecting ESI, *Inside Counsel*, October 16, 2012 (available at www.law.com/insidecounsel/sites/insidecounsel/2012/10/16/e-discovery-what-to-do-and-not-to-do-when-collecting-esi/).

§ 7.4:2 On-site Collections

On-site collections involve personnel visiting the client's physical location with special hardware and software that can create forensic images of computers. The identified custodians are scheduled to bring their laptops or make their computers available for imaging, and technical personnel perform their tasks carefully once the computer is provided. The technical personnel should document the procedure thoroughly by completing a chain of custody form, identifying the make and model of the computer, and taking adequate photographs of the serial number. Oftentimes the hard drive will be pulled for imaging, and once properly imaged and documented, the hard drive will be reinstalled on the computer.

Depending on the location of the individuals involved and the amount of data being collected, on-site collections can be an expensive proposition. It may involve considerable travel and personnel expenses since personnel must physically go to the client's location for the ESI collection. However, because the data is collected by experienced technical personnel, this option may provide the practitioner with peace of mind that the collection is done properly.

§ 7.4:3 Remote Collections Kits

Remote collection kits have become more common in recent times. This involves sending software, hardware, and detailed instructions to the custodian to assist in the data collection efforts. This kit will typically include a USB hard drive or other storage device so that the custodian can make a forensically sound copy of the ESI in just a few hours. Utilizing remote collection kits eliminates travel and other related expenses. They also include information to properly authenticate the data and document the procedure. This is a very good alternative to on-site collections because the collection is still being handled by experienced personnel, albeit remotely.

§ 7.4:4 Collections via Internet

ESI collection over the Internet is another form of remote collection. It involves the custodian installing software on the computer, after which the remote collection begins. However, in this instance, forensic images are sent via the Internet, which can result in slow and time consuming collections, depending on the size of the hard drive being imaged and limited Internet bandwidth. Thus, larger collections may lead to frustration by those involved due to the amount of time this process takes. This method of collection is only preferable for smaller data sets.

§ 7.4:5 Client Self-Collection

The final option for ESI data collection involves client self-collection. While this may often be the least expensive option and can be suitable for smaller collections, practitioners should be wary of permitting client-self collections in cases involving considerable volume of ESI or in instances where the client does not have the technical proficiency to adequately perform the self-collection. With this collection method, the client copies files to a hard drive or other media and delivers it to counsel. If the data needs to be received quickly, the client can also upload the data to an FTP site after converting the data to a ZIP file.

However, because these client self-collection efforts are left to the individual, it can be a risky endeavor since the employee may accidentally omit relevant information. Or, even worse, the employee may intentionally try to conceal relevant information they do not want to disclose.⁹ Furthermore, employees attempting to collect ESI may unintentionally alter the metadata and jeopardize the integrity of the ESI. While these dangers can be avoided with adequate preparation, planning, and education of the individuals collecting the data, practitioners must take considerable precautions to ensure that the ESI is collected in a manner that protects the integrity of the data.

§ 7.5 Collection Tips and Pitfalls

This section provides some helpful tips and pointers for effective document collection and also identifies some common dangers associated with the process.

- 1. E-mail should be collected using containers (e.g., PSTs¹⁰ or NSFs¹¹) so as to protect the integrity of the data, retain e-mail folder structure, and not alter the metadata.
- 2. Do not collect evidence through e-mail (i.e., do not let clients forward emails to you) because it alters the metadata.
- Use file copy software that can facilitate and expedite the process of copying files.

^{9.} See, e.g., GN Netcom, Inc. v. Plantronics, Inc., 930 F.3d 76 (3rd Cir. 2019) (involving company executives' act of deleting relevant e-mails and instructions to employees to do the same).

^{10.} A PST (personal storage table) is a Microsoft Outlook file that stores data from e-mail, contacts, and calendars.

^{11.} NSF files are files contained in Lotus Notes databases with the ".nsf" file extension.

- 4. Application data files should be collected preserving the original folder and file path to protect its integrity and to ensure functionality during the review process.
- 5. Assign evidence numbers to all data as it is collected for internal use in processing, review, and even invoicing (if passing the costs along to the client). Track the identity of custocians originally possessing the dataset and the source of the data for future reference.
- 6. Create an alias (i.e., assign a short name or custodian number that can be easily identified later) so that the actual custodian name is excluded from any searches in the dataset.
- 7. Beware of problems processing and reviewing Apple files and Microsoft Entourage e-mail and plan accordingly so that those files can be properly accessed and reviewed.
- 8. Plan for files that must be viewed in proprietary software (e.g., AutoCAD drawings, QuickBooks, Photoshop) to ensure full functionality and accessibility.
- 9. Be on the lookout for other technical issues, such as corrupt files, temporary files, links to files not collected, or foreign language documents that can affect the functionality and accessibility of the ESI.

§ 7.6 Conclusion

While ESI collection can be a daunting process, with proper planning and strategic implementation of a well-thought-out plan, it can become a manageable experience. A thorough and detailed investigation of the client's operations and technology practices will be invaluable to practitioners engaged in e-discovery. Practitioners should ask a lot of questions to obtain a full understanding of the universe of ESI that could be relevant to ongoing litigation. Attorneys who do not have a good grasp of all the potential electronic data that might pertain to a litigation matter are likely to have a hard time complying with their professional and ethical obligations to fully and completely participate in the discovery process. Completing a detailed investigation will provide the necessary foundation for the impending collection. Only then can practitioners have confidence that their ESI collection is thorough and comprehensive.

Table 7-1: Conducting IT/Technology Representative Interviews

- Document/Record Retention Policy
 - Does the company have one? If so, what is it?
 - Departing Employees:
 - □ What is the procedure for handling departing employees?
 - Are their computers preserved or wiped?
 - □ If preserved, relevant data must be produced.
 - □ What happens to their hard-copy files?
 - □ If preserved, relevant data must be produced.
 - Servers
 - Are there multiple office locations with different servers?
 - How many servers does the organization use?
 - □ What types of servers are used?
 - ☐ Are there dedicated servers for e-mail, shared drives, accounting, or other systems?
 - Does the organization use third-party service providers or cloudbased systems to store data?
- System Details
 - □ What type and version of operating system is used?
 - □ What e-mail system is used?
 - Do they have a network, and what information is stored on it?
 - Do they use webmail?
 - □ Do individuals have POP3 accounts (e.g., Google, Hotmail, Yahoo, or other such e-mail accounts)?
- Mobile Phones
 - Does the person/employee use a mobile phone?
 - Does the person/employee use more than one mobile device?

ESI Collection

- Does anyone else have access to the device? Need to consider possible uses by another party.
- □ Does the company have a "Bring Your Own Device" policy, or is the phone a personal one?
- □ Has the e-mail account otherwise been collected?
- □ Do text messages need to be collected?
- □ Are there instant messages on the mobile device that need to be collected?
- □ Is mobile phone data backed up in the cloud?
- Miscellaneous Considerations
 - □ What kind of equipment do individuals use (e.g., desktops, laptops, smart phones)?
 - Do individuals access social networks from company computers?
 - Does the organization utilize instant messaging?

□ If so, messaging logs must be retrieved.

- □ Is voice mail converted to WAV files?
- □ Is the organization recuired to save e-mail for a prescribed time period (e.g., energy traders or other regulated industries)?
- Does the organization have a disaster recovery plan?
- Do individuals have remote access to networks and other systems?
- Does the organization utilize special systems that must be planned for?
- Would connected home devices (e.g., Amazon's Alexa, Google Home, Apple HomePod) be helpful or have relevant data or information?
- □ Does the person use personal wearable devices? If so, could they contain helpful or relevant data or information?

Table 7-2: Conducting Individual Custodian Interviews

- Individual Workstations
 - Does the employee use a PC or Apple computer?
 - □ Is it a desktop, laptop computer, or both?
 - □ What is the make/model of the computer?
 - □ What operating system does the workstation use?
 - □ What is the size of the hard drive?
- Software
 - □ What software is used on a daily basis (e.g., Lotus Notes, Word, Excel)?
 - Does the employee use any specialty software (e.g., AutoCAD, Photoshop, QuickBooks)?
- Network Information
 - □ Is the individual's hardware connected to a network?
 - \Box If so, what city or office is the server located?

Relevant Data

- Does the custodian have relevant data?
 - □ In what form is the relevant data maintained (e.g., PST, OST, MSG, hard copy)?
 - □ If hard-copy data, where are the files stored or maintained?
- Data Storage and Backup
 - □ Where does the individual save data?
 - □ Is data saved locally on the computer?
 - □ Is it saved on a shared network?
 - □ Is it saved on a home directory?
 - Does the individual use thumb drives or other external drives?
 - Does the individual save data on a smartphone or PDA-like device?

ESI Collection

- □ What document management system does the individual use?
- □ Identify all databases that may contain potentially responsive data.
- □ Ascertain the path/folder name for potentially relevant data.
- Does the individual backup the computer locally?
 - □ If so, what type of media and software is used to backup the computer(s)?
- □ How long is backup data preserved?



Chapter 8

ESI Culling, Searching, and Reviewing

David J. Kessler, Keith M. Angle, and Alexander S. Altman

§ 8.1 Introduction

Civil discovery is the process of identifying information, documents, and data that are probative of the issues in dispute in the litigation. While discovery has many aspects and phases, they are all part of this process. Requesting parties serve document requests identifying the information they believe the other side has that is necessary for resolving the issues in dispute. Responses to such document requests identify what the responding party thinks the requesting party is entitled to and what it is willing to search for in offices and computer systems. Preservation is often about the identification of people and data stores that are likely to contain relevant information and taking reasonable steps to prevent the deletion or modification of such potentially relevant information.

At their essence, culling, filtering, search, and review are about the identification of specific relevant or responsive documents and segregating them from those documents that are irrelevant or nonresponsive. Traditional review involves lawyers or their agents manually reading and analyzing documents and determining their value to the matter: irrelevant, unresponsive, relevant, responsive, material, important, privileged, confidential, etc. Even in the digital age—even with technology-assisted review—review is still about lawyers analyzing documents and identifying the ones that matter. Now, however, technology allows lawyers to make decisions about more documents, more quickly, more consistently, and, with the right process and people, more effectively.

Moreover, culling and searching are two sides of the same e-discovery coin. With the explosion of information in the digital age, it has become practically impossible to review all documents and data by hand in order to identify what is relevant/responsive/material/important to the matter from one hard drive or one e-mail account or database, much less all the documents from all the potential computers and locations. In light of the renewed emphasis on proportionality, particularly in federal court and the December 1, 2015, amendments to Federal Rule of Civil Procedure 26(b)(1), this

is more true now than ever since reasonable searching and filtering may be the only way to cost effectively conduct discovery. Therefore, electronically identifying documents of interest ("searching") or electronically removing documents that are not of interest ("culling" and "filtering"), are a necessary and critical part of the discovery process in the electronic age.

§ 8.2 Culling and Searching Electronically Stored Information (ESI)

§ 8.2:1 Introduction

Like any aspect of discovery, culling and searching must be done in a reasonable manner. In essence, parties who use programmatic methods to identify relevant or responsive information must be reasonably certain that they do not exclude an unreasonable amount of data such that it is not produced or disclosed to their opponent or court. Moreover, a party should also consider that it does not want its search terms to identify an unreasonable amount of irrelevant or unresponsive data, as this will only clog the discovery process and unnecessarily drive up the cost of discovery. This tension between not excluding an unreasonable amount of relevant or responsive information (a.k.a. having reasonable "recall") and not including an unreasonable amount of irrelevant or unresponsive information (a.k.a. having reasonable "precision") defines a party's search and culling obligations and is the focus of the first half of this chapter.

§ 8.2:2 Culling and Searching in Service of Proportionality

The use of culling and searching speaks directly to the principle of proportionality in civil discovery. Although proportionality has long been considered in discovery, recent amendments to the Federal Rules of Civil Procedure have made the need for proportionality explicit. On December 1, 2015, the amended Fed. R. Civ. P. 26(b)(1) went into effect, explicitly requiring that all discovery be—

proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.¹

By employing the culling and searching techniques described below, producing parties can reduce the burden and expense of discovery. Conversely, requesting parties
can suggest culling and searching to recalcitrant responding parties as a means to reduce burden and expense, thus making the requested discovery more proportional and enabling requesting parties to obtain the information to which they are entitled. The cost of searching and culling—conducted well before review takes place—is marginal, but the benefits may be significant. These techniques, as described below, can significantly reduce the volume of ESI requiring review, creating substantial efficiencies and supporting proportionality. Moreover, by sampling and testing different techniques, responding parties can estimate the costs and benefits of tools and search words to more effectively meet and confer and, if necessary, raise proportionality arguments.

§ 8.2:3 Culling, Searching, and Reviewing in the E-Discovery Framework

The E-Discovery Reference Model (EDRM) illustrates the phases that typically make up the e-discovery process.² Culling and searching are not an explicit phase of e-discovery, like preservation, collection, or review, but can be an important component of many of the phases. In larger cases spanning many custodians, parties may use search terms to identify documents for preservation.³ Likewise, search terms can be used to collect documents, particularly from structured or semi-structured data sources like databases and websites.⁴ Parties can then search through their reviewed data to quality check the review and identify potentially privileged documents for secondary review and prevent inadvertent disclosure.

Where searching and culling are most commonly used is in "processing" between the time the data is collected from the parties' native IT environment and when the documents are reviewed. Reviewing documents manually is almost always the most expensive per-document expense and can be the most expensive phase of the EDRM lifecycle for any litigation. Thus, reducing the number of documents before review by using more economic means is crucial, but many parties do not have the IT infrastruc-

^{1.} Fed. R. Civ. P. 26(b)(1). A good discussion of the history of the amendments to rule 26(b)(1) can be found in Judge Conti's *Cole's Wexford Hotel, Inc. v. Highmark. Inc.*, Civ. A. No. 10-1609, 2016 WL 5025751 (W.D. Penn. Sep. 20, 2016) opinion.

^{2.} See, e.g., EDRM, EDRM Stages, www.edrm.net/resources/frameworks-and-standards/edrm -model/.

^{3.} See Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004) ("Zubulake V").

^{4.} See The Sedona Conference, Database Principles: Addressing the Preservation & Production of Databases & Database Information in Civil Litigation, 15 Sedona Conf. J. 171 (Sept. 2014), https://thesedonaconference.org/sites/default/files/publications/171-216%20Database%20Principles_0.pdf.

ture to conduct efficient and effective searches in their native environment and, thus, need to search and cull after they collect the data.

§ 8.3 Core Concepts

§ 8.3:1 Search

In the context of electronic discovery, "search" is the programmatic process of identifying documents or information a party is looking for in a population of documents and pulling them out for later review, analysis, and/or production. After a population of data has been identified as the likely source of desired documents or information, programmatic search is used to locate the specifically required data.

The vast majority of data searched in the e-discovery realm takes the form of documents containing text. To facilitate the search process, the text associated with document data is indexed before it is searched. The search tool or another software application is used to create a list of all words used throughout the documents in the data population and then catalogs where they occur. In searching data containing text, the most common search method is the use of keywords, either individually or in groups. When input into a search application, the keywords direct the application to identify the data containing, or excluding, specific text. While search is not the only tool for targeting relevant data, it remains the most prominent one in the world of ediscovery.

§ 8.3:2 Culling and Filtering

"Filtering" is a method of restricting data to predefined parameters. A common method of filtering is by using date filters. Restricting a data set by using date filters can be an effective way to quickly make an otherwise unwieldy set of data more manageable. Documents and other data may have a number of different date fields that can be filtered. E-mails can be sorted by the date sent. Word processing and spreadsheet documents often have creation dates, modification dates, and even dates tracking when different drafts were saved. If a litigant knows that the opposing party generated relevant documents over a specified time period, date filters can make quick work of targeting the most useful data population.

"Culling" is the programmatic process of identifying nonresponsive or otherwise nondiscoverable documents or data and removing it from the data population. In this sense, it is the flip side of search, and many of the same techniques used to locate responsive data can be used to cull nonresponsive data. The purpose of programmatic culling is to winnow down an initial data population to a more manageable and focused set of documents and information. To draw an analogy, consider the final, desirable set of responsive data a sculpture and the nonresponsive data the marble that must be carved away to get to the final work of art.

Given the explosive growth of electronic information, filtering and culling are critical steps in making the entire discovery process more efficient.

§ 8.4 Role in the Discovery Process

§ 8.4:1 Reduce Overall Volume

More than 93 percent of information now manifests itself as ESI, and the average business person generates 2.5 gigabytes of ESI annually.

§ 8.4:2 Reduce Time and Costs Associated with Reviewing Irrelevant Data

With the increasing amount of storage capacity available, the tendency to use the email inbox as a filing cabinet increases, resulting in a data warehouse on every desk. For the user, there may be no affirmative act required to keep data; instead, an affirmative act is generally required to destroy the data.

§ 8.4:3 Focus Review on Relevant Data

According to a Rand Corporation study, document review accounted for at least 70 percent of the total costs of document production.⁵ The culling of ESI begins at the earliest stages of discovery by identifying relevant sources of information, key custodians, critical dates, and a plan for managing the discovery process. Culling continues throughout the discovery process, occurring at multiple stages and likely relying on various methodologies.

^{5.} Nicholas M. Pace and Laura Zakaras, *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*, RAND Institute for Civil Justice (2012), www.rand.org/ content/dam/rand/pubs/monographs/2012/RAND_MG1208.pdf, p. 21 fig. 2-2.

§ 8.5 General Concepts

This section analyzes some of the basic, high-level concepts that generally apply to the searching and culling process. In the following section, the specific methods available to assist counsel and their clients in searching for and identifying documents are analyzed.⁶

§ 8.5:1 Precision and Recall

The concepts of precision and recall are related and are based on measures of relevance to the search being conducted. Precision is the fraction of retrieved documents identified as relevant by a search or document review.⁷ Recall is the fraction of relevant documents that are retrieved by a search or document review.⁸ In simple terms, high recall means that a search engine returned most of the relevant results, while high precision means that the search returned substantially more relevant results than irrelevant. For example, perfect precision is achieved when a search brings back one relevant document, and perfect recall is achieved when a search returns the entire document population.

Often, there is an inverse relationship between precision and recall where it is possible to increase one at the cost of reducing the other. At one extreme, 100 percent recall could be achieved by a search that returned the entire document population,⁹ but precision would be low. At the other extreme, 100 percent precision could be achieved by a search that returned a single relevant document, but recall would be low. More generally, a broader search returning many documents will have higher recall and lower

^{6.} See Maura R. Grossman and Gordon V. Cormack, *Glossary of Technology-Assisted Review*, Fed. Cts. L. Rev. 1 (2013), www.fclr.org/fclr/articles/html/2010/grossman.pdf (listing of definitions of the technical terms and concepts used in searching and culling solutions); see also The Federal Judge's Guide to Discovery, *The Use of Advanced Technologies in Document Review*, The Electronic Discovery Institute, p. 80 2d ed. (2015).

^{7.} See Grossman & Cormack, at 25 ("precision" defined). A value can be assigned to precision using the number of relevant documents retrieved by a search, divided by the total number of documents retrieved by that search. A perfect precision score of 1.0 means that every result retrieved by a search was relevant (but says nothing about whether all relevant documents were retrieved); see also The Federal Judge's Guide to Discovery, *The Use of Advanced Technologies in Document Review*, p. 80.

^{8.} See Grossman & Cormack, at 27 ("recall" defined). A value can be assigned to recall using the number of relevant documents retrieved by a search divided by the total number of existing relevant documents (even those not retrieved). A perfect recall score of 1.0 means that all possible relevant documents were retrieved by the search (but says nothing about how many irrelevant documents were also retrieved; see also The Federal Judge's Guide to Discovery, *The Use of Advanced Technologies in Document Review*, p. 80.

^{9.} See Grossman & Cormack, at 14 ("document population" defined).

precision, while a narrower search returning fewer documents will have lower recall and higher precision.

§ 8.5:2 False Positive

A false positive is a nonrelevant document that is incorrectly identified by the search method as a relevant document.¹⁰

§ 8.5:3 False Negative

A false negative is a relevant document that is incorrectly identified by the search method as a nonrelevant document.¹¹

§ 8.5:4 Hit Report

Search solutions will typically provide the user with a report that indicates the number of documents containing relevant search terms and the number of times the search terms appear in each document. This report identifies the quantity of the documents identified by the search terms, but generally provides no details as to the quality of the search terms (e.g., did they identify relevant documents?).

§ 8.5:5 Technology-Assisted Review (TAR)

Technology-assisted review, or TAR, is a term that covers the technology tools described in this chapter to make document search and review more accurate and cost effective. Such tools include data analytics, which identify metadata such as dates, file type, and file size, as well as concept grouping or clustering, discussed below. TAR also refers to predictive technologies, which consist of tools that prioritize or code a collection of documents using a computerized system that harnesses human judgments of one or more subject matter expert(s) on a smaller set of documents and then extrapolates those judgments to the remaining document collection.¹² Some such methods use machine-learning algorithms that "learn" which documents have been coded "relevant" and "nonrelevant" by human reviewers, and can then find more doc-

^{10.} See Grossman & Cormack, at 16 ("false positive" defined); see also The Federal Judge's Guide to Discovery, The Use of Advanced Technologies in Document Review, p. 80.

^{11.} See Grossman & Cormack, at 16 ("false negative" defined).

^{12.} See The Federal Judge's Guide to Discovery, The Use of Advanced Technologies in Document Review, p. 74–77.

uments like those already coded. Other methods derive systematic rules that emulate expert decision-making. Predictive TAR processes generally incorporate statistical models and/or sampling techniques to guide processes and measure overall system effectiveness.¹³

§ 8.5:6 Sampling

Sampling refers to a subset of a document population used to assess some characteristic of that population.¹⁴ A random sample, for example, is a subset of a document population derived using a method that is equally likely to select any document from the population for inclusion in the sample. Samples are typically used to calculate and assess a statistical estimate of the reliability and accuracy of the search terms or methods employed.

§ 8.6 Searching and Culling Methods and Techniques

§ 8.6:1 Traditional "Hands-On" Review

Commonly referred to as "linear review" is the nonautomated practice where lawyers, usually junior associates, perform a manual review of all potentially responsive documents.¹⁵ Each document is reviewed for relevance and privilege, often by multiple lawyers. Although linear review is not a computer-assisted method of review, a party will often test for quality using random sampling and subsequent review by more senior lawyers.

Linear review has the benefit of assuring that every potentially responsive document is scrutinized by at least one attorney, thus reducing the likelihood that the final production will be challenged in court. On the down side, linear review can be time consuming and extremely expensive, particularly with large troves of electronically stored information. Moreover, evidence is mounting that linear review is inferior to automated methods in terms of precision, recall, and accuracy. While these risks can be mitigated by using more experienced lawyers, this only increases the expense of review.

^{13.} For further explanation of technology assisted review, see Chapter 10—Predictive Coding and Computer-Assisted Document Review.

^{14.} See Grossman & Cormack, at 29 ("sampling" defined).

^{15.} See Grossman & Cormack, at 22 ("linear review" defined).

§ 8.6:2 System File Filtering

System file filtering is a culling method that scours the universe of potentially responsive data and removes operating system files, executable files, and other ancillary files used in the operation of software. Except in rare cases, these files are unlikely to have information supplied by data custodians.

System file filtering is a simple way to improve subsequent review methods by reducing the volume of electronic data files requiring review. System file filtering may not be appropriate, however, where such files would contain potentially responsive data. For example, in patent prosecution cases where software development is at issue, system file filtering may pose an unacceptable risk.

§ 8.6:3 Deduplication

Deduplication is the process of culling duplicate data files from the universe of potentially responsive data.¹⁶ How duplicates are identified depends on the e-discovery service provider and its proprietary tools. The obvious benefit is that deduplication can drastically reduce the volume of files requiring further review. If not carefully developed and configured, however, deduplication runs the risk of removing potentially relevant files from the data universe. For example, two files may contain the same content but have different metadata that may be of great value.

§ 8.6:4 Metadata and Date Filtering

Electronic documents consist of more than their textual or graphic contents. Most data files have metadata, sometimes called "data about data," associated with them. Details such as creation and modification dates, authors, and system details and versions lie embedded in the software code of many documents. Most electronic discovery tools search through these hidden fields of data as well as the main content of data files. One important means of searching and culling data is the use of data filtering, and the metadata of most documents makes this possible through a quick and efficient process. By setting date parameters, the volume of files to be reviewed can be quickly winnowed down to only those that fit within a reasonable range. Creation dates, modification dates, and even version dates of documents may be used to perform filtering. While this can help weed out many irrelevant documents, counsel must carefully determine the correct date ranges to avoid culling out potentially relevant documents.

^{16.} See Grossman & Cormack, at 14 ("decuplication" defined).

§ 8.6

§ 8.6:5 Keyword Searching

The most common means of searching electronically stored information has traditionally been via keyword. Keywords are often coupled with instructions—expanders or limiters—to ensure that the scope of data returned is neither too broad nor too narrow. For example, a search of a data set using the keyword "claim" would only return those documents containing the exact word "claim." However, a search using the term "claim*" would likely return a larger set of documents, with the words "claim," "claimant," "claiming," "claimed," and "claims" all meeting the search criteria. Alternatively, one could construct the search terms to include "claim," but not "claimant," thus returning a more limited and possibly more manageable set of documents. Certain classes of search terms are common in e-discovery, such as the names of key players in the litigation, specific internet domain names, product names, and document categories. Obviously, the application of keywords in cases involving non-text data (e.g., images, schematics, video) is limited. Keywords may still have some use, however, as such files usually have text-based file names that can be searched.

One or more parties to a litigation will determine a list of words that they would expect to find in responsive, text-based documents. The electronic discovery vendor or forensic team can then programmatically search the data universe for matching documents. Keyword searching can be highly effective if the parties take care in developing keyword lists. However, careless keyword development without consulting custodians, IT professionals, and others with specific knowledge of the documents and data systems being searched can cause a party to overlook a large volume of responsive documents. Moreover, keyword searches are largely unviable for non-text files such as images, audio, and video.

"Keyword searching" is a simple term that encompasses various search methods and techniques. Some of the most common techniques are described below.

Simple: A simple keyword search is conducted by merely looking for specific words or phrases in the documents comprising the data universe. For example, if the litigation concerns a product called a "widget," the search tool may be programmed to find all files containing the word "widget." Other simple keywords might be the names of key players, technical terms, project names.

Boolean: A Boolean search allows a party to apply a logical identifier to one or more keywords to obtain more accurate results. For example, if the litigation concerns a product called "Alpha widget," the search tool could be configured to find all files containing the word "alpha" and the word "widget," even if they do *not* appear next to

each other. Similarly, the tool could be configured to find only those files where the word "beta" does not appear. Multiple Boolean expressions can be used in the same search to target highly specific sets of data.

Wildcard: A "wildcard" is a means of searching for multiple variations of a keyword. The characters "*" or "!" function as wildcards in most search tools. For example, searching for the word "litigation" might produce a relatively small volume of documents. By applying a wildcard and searching for "litig*," the search tool would return documents containing "litigate," "litigation," "litigant," and "litigious."

Stemming: Stemming is a means of reducing a keyword to its "stem" and then searching for any expanded words based on the stem. For example, if the keyword "synchronize" were supplied to a search tool employing stemming, it would treat the letters "chron" as the stem and search for documents containing the words "chronic," "chronometer," or "chronograph."

Complex: Obviously, no single keyword search technique needs to stand alone. Highly complex searches can be designed using Boolean connectors, wildcards, and stemming to arrive at more precise results. Caution must be used, however, as poorly designed complex searches can be wildly over- or under-inclusive.

§ 8.7 Benefits and Limitations of Search

The benefits of electronic search and culling are easily stated. Used properly, search and culling allows for a lawyer to either focus in on documents and data most likely to be relevant or responsive, or to discard data that is not reasonably likely to contain relevant information. Just as attorneys have been doing for decades at the macro level, by focusing on relevant departments, people, offices, and filing cabinets and avoiding irrelevant departments, people, offices, and filing cabinets, electronic search and culling allows lawyers to make these decisions at an electronic file level *without having to review each file by hand*.

The limitations of search may not be as obvious. First, a document needs to be searchable in order to be identified. Keyword search will not identify documents without significant text, pictures, audio files, and TIFF files. Second, the quality of the searchable text will impact the quality and efficacy of the search. Documents that have been scanned and from which searchable text has been generated by an optical character recognition (OCR) process¹⁷ may have significant errors depending on the quality of

^{17.} See www.edrm.net/glossary/ocr/.

the original text and the quality of the OCR engine. This could downgrade the quality of the search. Likewise, a search by the "author" of a document may not be particularly effective if, for example, the word processing program labels all documents with the ex-CIO's name as author. This is a classic "garbage in/garbage out" ("GIGO") problem, where the ability of a party to search its documents is dependent on the quality of the underlying information in the first place. Third and finally, not all search programs and tools are created equal. How and where they search (and how much of a document or database they search) can vary widely from tool to tool. Before using any search tool, an attorney should become reasonably familiar with it to make sure it will do a reasonable job at what it is being asked to do. It may be necessary for counsel to engage an IT or search consultant to help the lawyer evaluate the search tool and the quality of the search he or she is attempting to conduct.

§ 8.8 Other Search Methods and Techniques

In addition to keyword searching, some technologies offer automated processes to help attorneys prioritize the review process.

§ 8.8:1 Similarity Grouping or Clustering

Some solutions involve finding related documents by using proprietary algorithms that recognize patterns indicating similarities among the documents and "cluster" them into groups. Documents are segregated into categories or groups with the goal that the documents in any group are more similar to one another than to those in other groups.

Similarity grouping or clustering is performed automatically by the computer system and involves no human intervention, so the process can be fast and cost-effective. Some systems perform the grouping behind the scenes as the data is loaded into the document review platform and pose a low impact on the time it takes to process the information. If the results are as expected, the grouping can greatly improve the efficiency of the review process, because related documents can be assigned to the same reviewers for faster and more consistent coding and tagging. Clustering is not always reliable, however, and depending on the document population, the resulting categories may or may not reflect distinctions that are valuable for the purpose of a search or review effort.

§ 8.8:2 Concept Searching

A concept search (or conceptual search) is an automated information retrieval method that is used to search electronically stored unstructured text (e.g., digital file archives, e-mail, network file directories) for information that is conceptually similar to the information provided in a search query. In other words, the ideas expressed in the information retrieved in response to a concept search query are relevant to the ideas contained in the text of the query. Concept searches return documents sorted and ranked by relevance and identify documents that would not be returned by a simple keyword or Boolean search.

Concept search methods range from simple techniques to find variations or synonyms of the original keyword to advanced statistical algorithms, such as latent semantic indexing, that go beyond synonym or keyword matching to include all documents that describe the same subject matter or concepts regardless of the specific terms or words used. For example, concept searching understands that the words "terminate" and "fire" and also the phrase "end association with" describe the same idea or meaning, and would exclude results related to combustion activities.

By using full-text, natural language that is similar to what is likely to be contained in the documents sought, concept searching can find documents that contain similar ideas to those expressed in the search query. Concept searches should not be affected by misspelled words or typographical errors in either the query or the documents themselves.

The more advanced concept searching methods generally result in finding more relevant documents than simple keyword or standard Boolean searching. If a query is carefully crafted to include enough text to convey the concept while keeping the query focused on one particular concept, then resulting document groups can be strongly connected, allowing attorneys to review the documents most likely to be relevant at an earlier time in the review. As with clustering, the quality of the results will depend on the document population. Unlike clustering, however, which is an automated process, concept searching is also dependent on the accuracy of the terms and phrases that are the basis for the search. A number of iterations may be needed to refine the queries to obtain more relevant results.

§ 8.8:3 Visual Mapping

Tools are available to graphically depict the results of searches, clustering, and concept grouping. One useful tool is software that displays related e-mail messages by recipient, sender, and keywords or concepts in a spoke-and-wheel format; this depiction allows counsel to quickly identify who was communicating with whom about a topic and the relative frequency of the communications, making it possible to identify custodians who may have been overlooked and prioritize the custodians who have the most message traffic.

§ 8.9 Searching and Culling Standards

§ 8.9:1 Statutory and Regulatory Guidelines

The Texas Rules of Civil Procedure that govern the scope and limitations of discovery are similar to the Federal Rules of Civil Procedure. Tex. R. Civ. P. 192.3(a) governs the broad scope of discovery and provides for the discovery of documents that are not privileged and are relevant to the subject matter of the pending action. Tex. R. Civ. P. 192.3(b) provides for the discovery of documents, defined to include "data, and data compilations," the same terms used in the federal rules before the 2006 amendments. Tex. R. Civ. P. 192.3 provides for proportionality in discovery and allows courts to limit discovery if the burdens or expenses outweigh the likely benefit. As of this writing, the Texas rules have not been amended to mirror the 2015 amendments to Fed. R. Civ. P. 26(b)(1), which explicitly proscribe the scope of discovery in terms of proportionality.

The Texas rules do not address how or to what extent search techniques and methodologies should be used in the discovery process. The Texas Supreme Court has, however, instructed that the Texas rules governing discovery (including electronic discovery) are sufficiently similar to the federal rules so that Texas courts can look "to the federal rules for guidance."¹⁸ Fed. R. Civ. P. 26(b)(2)(B) defines specific limitations on the frequency and extent of the discovery of electronically store information, including information that is not reasonably accessible because of undue burden or cost. The Texas analog is rule 196.4, which requires a party to produce ESI responsive to the request that is reasonably available to the responding party in its ordinary course of business.

§ 8.9:2 Case Law

Unfortunately, there is a dearth of case law in Texas and in the Fifth Circuit regarding searching, culling, and how to reasonably develop and implement search terms. That

^{18.} In re Weekley Homes, L.P., 295 S.W.3d 309, 317 (Tex. 2009) (orig. proceeding).

ESI Culling, Searching, and Reviewing

being said, there are several federal cases, discussed below, that are useful in understanding how parties should approach search and their obligations in creating a reasonable search and cull process.

One the leading cases on the use of search terms in discovery is *Victor Stanley, Inc. v. Creative Pipe, Inc.*¹⁹ While search term issues had been addressed by courts previously,²⁰ Judge Grimm's *Victor Stanley* opinion was a turning point in how courts looked at search terms and whether a party's conduct was reasonable.

Before discussing the opinion and what it can teach, it is important to note a few unique things about this case that differentiate it from the standard search term case. First, the primary issue in this case was whether defendants had waived their privilege by inadvertently disclosing privileged documents to the plaintiffs. The question was whether the defendants' use of search terms to identify privileged material was a "reasonable precaution" to avoid inadvertent disclosure. Thus, unlike in most discovery cases where the opponent has to show the use of search terms was unreasonable (as they have the burden on a motion to compel or for sanctions), in *Victor Stanley* the user of search terms had the burden to show their use was reasonable. Moreover, this required the party to disclose the search terms it used in order to meet its burden.

While the parties disagreed about how defendants reviewed for privilege, the defendants asserted that after the joint ESI search protocol was implemented and responsive ESI identified, their computer forensics expert conducted a privilege search using approximately seventy keyword search terms. The potentially privileged documents were segregated and provided to defense counsel "for the first phase of the pre-production privilege review."²¹ The privilege keyword search was performed on those ESI files (4.9 gigabytes) that were in text-searchable format. For the other ESI files that were not in text-searchable format (33.7 gigabytes), defense counsel and an individual defendant stated they performed a manual privilege review. This "second phase" of the privilege review was a page-by-page review; however, "due to the compressed schedule and time constraints in reviewing these tens of thousands of documents within the time permitted, this review was undertaken by reviewing the page titles of the documents."²²

- 21. Victor Stanley, 250 F.R.D. at 256.
- 22. Victor Stanley, 250 F.R.D. at 256.

^{19. 250} F.R.D. 251 (D. Md. 2008).

^{20.} See, e.g., Qualcomm Inc. v. Broadcom. Corp., No. 05cv1958-B (BLM), 2008 WL 66932 (S.D. Cal. Jan. 7, 2008).

The court was not impressed with either the defendants' description of their search or, based on what it did disclose, what defendants actually did:

First, the Defendants are regrettably vague in their description of the seventy keywords used for the text-searchable ESI privilege review, how they were developed, how the search was conducted, and what quality controls were employed to assess their reliability and accuracy. While it is known that M. Pappas (a party) and Mohr and Schmid (attorneys) selected the keywords, nothing is known from the affidavits provided to the court regarding their qualifications for designing a search and information retrieval strategy that could be expected to produce an effective and reliable privilege review. As will be discussed, while it is universally acknowledged that keyword searches are useful tools for search and retrieval of ESI, all keyword searches are not created equal; and there is a growing body of literature that highlights the risks associated with conducting an unreliable or inadequate keyword search or relying exclusively on such searches for privilege review. Additionally, the Defendants do not assert that any sampling was done of the text searchable ESI files that were determined not to contain privileged information on the basis of the keyword search to see if the search results were reliable. Common sense suggests that even a properly designed and executed keyword search may prove to be over-inclusive or under-inclusive, resulting in the identification of documents as privileged which are not, and non-privileged which, in fact, are. The only prudent way to test the reliability of the keyword search is to perform some appropriate sampling of the documents determined to be privileged and those determined not to be in order to arrive at a comfort level that the categories are neither overinclusive nor under-inclusive. There is no evidence on the record that the Defendants did so in this case. Rather, it appears from the information that they provided to the court that they simply turned over to the Plaintiff all the text-searchable ESI files that were identified by the keyword search Turner performed as non-privileged, as well as the non-text searchable files that Monkman and M. Pappas' limited title page search determined not to be privileged.²³

Judge Grimm's analysis focuses on the question of what the search terms are failing to identify (i.e., what documents of interest are they not hitting on). In the *Victor Stanley* case, what information did defendants have that their search terms would identify a

^{23.} Victor Stanley, 250 F.R.D. at 256-57 (emphasis added).

reasonably sufficient number of the potentially privileged documents? The only way to determine this question, Judge Grimm concludes, is for the party to conduct some reasonable investigation into the documents and data that the search terms do not "hit." Thus, to determine the quality of the search terms and to see if they are doing a reasonable job of identifying all documents within the scope of the search, a party should sample the documents that are not selected by the search terms.²⁴ Judge Grimm does not provide a bright-line rule to determine when a search is reasonable or when a search has missed an unreasonable number of documents. Nor does Judge Grimm address how to balance a party's desire to identify documents of interest when selecting too many irrelevant documents and unreasonably increasing the cost of review.

Another useful case related to search is *William A. Gross Construction Associates, Inc. v. American Manufacturers Mutual Insurance Co.*,²⁵ which discusses the recurring theme of cooperation among parties when identifying search terms. In the *Gross* case, Judge Peck stated that cooperation among the parties on search techniques is the best way to avoid disputes as to the scope and quantity of search terms to cull ESI. The judge put practitioners in the Southern District of New York on notice that "careful thought, quality control, testing, and cooperation with opposing counsel" should guide parties when designing search terms for the production of ESI.²⁶ More specifically, the court cautioned against the practice of litigants and lawyers unilaterally establishing search terms.²⁷

In the case of *In re Broiler Chicken Antitrust Litig.*, No. 1:16-cv-08637, 2018 WL 1146371 (N.D. Ill. Jan. 3, 2018), Magistrate Judge Jeffrey Gilbert approved a consent order set forth by appointed Special Master Maura Grossman and agreed to by all the parties that required the parties to engage in a highly transparent process of identifying and reviewing documents through keyword searches or TAR. The special master opined that it was crucial for producing parties to be transparent and cooperative and to disclose a myriad of details regarding search terms and the use of TAR, such as descriptions of search software and the software's default stop and noise words, the name of the party's TAR vendor, a description of the TAR process and how it works,

^{24.} Victor Stanley, 250 F.R.D. at 257. See also City of Rockford v. Mallinckrodt ARD Inc., 326 F.R.D. 489, 494 (N.D. Ill. 2018) ("[S]ampling the null set when using key word searching provides for validation to defend the search and production process").

^{25. 256} F.R.D. 134 (S.D.N.Y. 2009).

^{26.} Gross, 256 F.R.D. at 134.

^{27.} While not specifically requiring parties to use expert testimony to establish the adequacy of search terms, Judge Peck held that "something other than a lawyer's guesses, without client input, and without any quality control testing" would have to inform the process of culling ESI through the use of search terms. *Gross*, 256 F.R.D. at 136 n.3.

information on how the party trains the TAR algorithms, and the producing party's quality control measures. Under the protocol, after conducting a sample of the results, the parties would provide a table of each document and its coding and a copy of each responsive, non-privileged document to the receiving party and to the special master. This level of transparency and detailed disclosure is not typical, and it is unclear that a court could order such a protocol over the objection of the parties under either federal or Texas rules of civil procedure (see the discussion of search terms as work product below).²⁸

In the case of In re Biomet M2a Magnum Hip Implant Products Liability Litigation,²⁹ instead of disputing the adequacy of search terms, the plaintiffs disputed whether keyword searches should have been used at all to cull and find electronic documents. Facing numerous decentralized cases, defendant Biomet conducted keyword searches of nearly 20 million documents in furtherance of its discovery obligations. Biomet then employed predictive coding on the resulting set to arrive at 2.5 million responsive, relevant documents. At that point, Biomet had incurred over one million dollars in ediscovery costs. A steering committee of centralized plaintiffs objected to this methodology, arguing that the initial use of keyword searches was unreliable and rendered the use of predictive coding on the resulting set flawed. The steering committee urged the court to compel Biomet to go back and use predictive coding to identify responsive documents from the original 20 million document set. Judge Miller refused to decide whether predictive coding was superior to keyword searching. Citing the proportionality standard in Fed. R. Civ. P. 26(b)(2)(C)(iii), Judge Miller held that the burden and expense requiring *Biomet* to recommence discovery outweighed its likely benefit to the plaintiffs.³⁰ Instead, Judge Miller sounded a familiar refrain and urged cooperation between the parties to establish search terms to be used on the culled set of documents.31

Although parties should be cautious when unilaterally developing and deploying search terms without first taking steps to verify their accuracy and efficacy (a process often referred to as "search term calibration"), in the case of *United States v. O'Keefe* the court rejected a challenge to a party's use of search terms without a specific evi-

^{28.} It should be noted that while courts encourage transparency in discovery practices, requiring parties to engage in this level of disclosure of their internal procedures is not traditional, as courts "[are] not normally in the business of dictating to parties the process that they should use when responding to discovery." *Rio Tinto PLC v. Vale S.A.*, 306 F.R.D. 125, 127 (S.D.N.Y. 2015) (quoting *Dynamo Holdings L.P. v. Comm'r*, 143 T.C. 183, 188 (2014)).

^{29.} No. 3:12-MD-2391, 2013 WL 1729682 (N.D. Ind. Apr. 18, 2013).

^{30.} Biomet, 2013 WL 1729682, at *3.

^{31.} Biomet, 2013 WL 1729682, at *3.

dentiary showing under rule 702 of the Federal Rules of Evidence that the search terms used were inadequate.³² The issues were raised in the context of a criminal matter, and the court turned to the Federal Rules of Civil Procedure for guidance. Judge Facciola observed that "for lawyers and judges to dare opine that a certain search term or terms would be more likely to produce information than the terms that were used is truly to go where angels fear to tread."³³ To successfully challenge a responding party's production of ESI, the court stated that the requesting party must do more than speculate that additional search terms would yield more responsive results.

In the case of National Day Laborer Organizing Network v. U.S. Immigration and Customs Enforcement Agency,³⁴ a Freedom of Information Act (FOIA) action, the court highlights the dangers that arise when a responding party fails to conduct keyword searches of ESI methodically. Responding to a FOIA request, several federal agencies, including the FBI and the Department of Homeland Security, relied on custodians of ESI to conduct keyword searches to find responsive documents. Each responding agency, however, differed in its methodology-some supplied custodians with "suggested" search terms, others required that specific search terms be used by custodians, and in the FBI's case, the court was given no indication at all which search terms were used. In FOIA cases, the government must show that its search for documents was adequate. Where keyword searches are concerned, Judge Scheindlin first observed that a court cannot determine the adequacy of a FOIA response if the government does not state which search terms and methodologies were used. Judge Scheindlin went on to opine that keyword searches of ESI performed by the custodians themselves were likely to be inadequate because, while the use of keyword searches has become routine for almost anyone creating or possessing ESI, complying with FOIA requests poses unique challenges: "Searching for an answer on Google is very different from searching for all responsive documents in the FOIA or e-discovery context."35 Lastly, Judge Scheindlin noted that keyword searches of ESI may be highly flawed and may be inadequate when emerging methodologies such as predictive coding are becoming more reliable. In crafting an order, Judge Scheindlin ultimately urged cooperation between the parties to determine the best search terms and methodologies.

34. 877 F. Supp. 2d 87 (S.D.N.Y. 2012).

35. National Day, 877 F. Supp. 2d at 108.

^{32.} United States v. O'Keefe, 537 F. Supp 2d 14, 24 (D.D.C. 2007).

^{33.} O'Keefe, 537 F. Supp. 2d at 24.

§ 8.9:3 Proportionality and Search

While the case law above does not directly address proportionality (*Victor Stanley* comes the closest), the lesson from all these cases is that reasonable search and filtering tools and techniques are well-established parts of a good discovery process. By sampling and testing search terms and other tools that return estimated recall and precision levels, responding parties can better measure the expected effectiveness and efficiency of their protocol. For example, if an opponent suggests a new search term, does it improve recall? That is, will it bring back new responsive documents that previous searches failed to identify? Also, what is the effect on precision? Does it bring back many nonrelevant documents from the sample and therefore increase the expected amount of irrelevant documents that will need to be reviewed? By looking at the benefits (or harm) of broadening (or narrowing) a search and comparing it to the increase (or decrease) in the expected cost of review, the parties and the court can better judge if the search was reasonable *and proportionate*.

§ 8.10 Other Uses of Search in Discovery

§ 8.10:1 Identification of Privilege

In addition to helping a user find relevant documents and eliminate nonrelevant documents, keyword searching can assist attorneys in identifying privileged information by finding the names of law firms, attorneys, law firm e-mail addresses, and words commonly associated with privileged communications, such as "attorney-client" and "privilege." Similarly, by working with custodians who have knowledge about the business operations, attorneys can craft keyword searches to identify confidential and trade secret data associated with an organization's valuable business information. The use of predictive technologies can also help counsel identify privileged documents by having the system look for documents that are similar to those coded as privileged by the reviewing attorneys. As noted above in the discussion of the *Victor Stanley* case, reliance on key terms to identify privileged documents should be supported by quality control processes that assess the reliability, accuracy, and reasonableness of the terms used. Privilege waiver is discussed in greater depth in chapter 10 of this book.

§ 8.10:2 Search Terms as Work Product

Under Texas law, work product is defined as-

172

- 1. material prepared or mental impressions developed in anticipation of litigation or for trial by or for a party or a party's representatives, including the party's attorneys, consultants, sureties, indemnitors, insurers, employees, or agents; or
- 2. a communication made in anticipation of litigation or for trial between a party and the party's representatives or among a party's representatives, including the party's attorneys, consultants, sureties, indemnitors, insurers, employees, or agents.³⁶

Such work product material is either not discoverable, if it is core work product, or can only be discoverable if the other party can show a "substantial need" and cannot obtain the materials elsewhere without "undue hardship."³⁷

Thus, even if search terms were considered relevant under Texas law, which is arguable as they are not probative of any issue on the merits, it is clear that most of the time they would be considered work product as they are almost always prepared in anticipation of litigation by a party's attorneys. While there is no case exactly on point, the Texas Court of Appeals did address an analogous issue in *In re Exxon Corp.*, 208 S.W.3d 70 (Tex. App. 2006). In *In re Exxon*, plaintiffs wished to depose a corporate representative of Exxon who could explain "the process by which Exxon's representative responded to requests by production."³⁸ As the court found: "this subject necessarily and almost exclusively concerns the 'mental impressions developed in anticipation of litigation or for trial by or for a party or a party's representative."³⁹ As search terms are a crucial aspect of how a party identifies documents to respond to document requests, the court's logic in *In re Exxon* would appear to find search terms nondiscoverable.

This does not mean that parties cannot choose to waive the work product protection and exchange search terms or other culling and filtering tools. There are numerous reasons why parties could decide that it is in their own best interest to disclose the search terms they are using to their opponents or get their opponent's input on how they are conducting their search. It simply appears they cannot be forced to do it under Texas law absent concrete evicence of a discovery failure (parties would be wise to prepare to waive certain protections in order to use their discovery process to defend their production).⁴⁰

- 37. See Tex. R. Civ. P. 192.5(b)(1), (b)(2).
- 38. 208 S.W.3d 70, 75.
- 39. In re Exxon Corp., 208 S.W.3d at 75 (quoting Tex. R. Civ. P. 192.5(a)(1)).

^{36.} Tex. R. Civ. P. 192.5(a).

§ 8.11 Review of Electronically Stored Information

§ 8.11:1 Overview

Document review is the process used to review the documents in a culled data set to identify responsive documents to produce, documents to support defense efforts, and privileged and confidential documents to withhold. A legal team uses the document review process to gain a greater understanding of the factual issues in a case and applicable legal strategy based on the type of information that is found in the collection of documents. Outside of issues related to privilege, there is a dearth of case law because there is nothing to audit. Courts appear to presume that if a reasonably informed person looks at the documents, they will identify those that are responsive.

§ 8.11:2 Review Process

The document review process represents a core component of contemporary legal projects and is used to identify material relevant to the matter as well as privileged and confidential material meriting additional safeguards and protection. The appropriate process is crucial to provide the attorney with a framework to efficiently review documents and thereby gain a more comprehensive understanding of the legal and factual issues associated with the matter.

The exploding volume of ESI and the related costs of reviewing this material requires attorneys to put careful thought into the staffing, resourcing, and organization of any document review project. To establish an effective review process, attorneys must understand the scope of the review project, select the vendors and technologies best suited to handle the needs of the project, and properly prepare the review team. Likewise, attorneys must establish an effective management system to oversee and evaluate the performance of the review team.

In this section, we will outline the critical elements attorneys must consider in the organization of a document review project.

^{40.} The Sedona Conference, Commentary on Defense of Process Principles and Guidelines for Developing and Implementing a Sound E-Discovery Process (2016), www.ediscoverycouncil.com/sites/ default/files/The%20Sedona%20Conference%20Commentary%20on%20Defense%20of %20Process_Public%20Comment%20Version_Sept%202016.pdf.

§ 8.11:3 Develop Review Strategy for Project

The rapidly expanding volume of ESI generated by individuals and corporations makes it difficult to review each document collected by attorneys for relevance, responsiveness to discovery requests. and privileged and/or confidential material. Attorneys should take steps to control the scope of the review project to allow the efficient identification of the desired information. The strategic collection and selective filtering of data using date ranges is one method of controlling the scope of review. Additionally, attorneys should make effective use of federal rule 26(f) conferences with opposing counsel to discuss and agree upon the scope (e.g., custodians, key material, geographic scope, and temporal scope).

Review Protocols and Guidance Materials: Once scope is established, develop protocols and documentation to guide the review project. The manager selected to oversee a project must understand the matter and the related factual and legal issues. Guidance materials must be clear and well-organized, provide background on the matter, identify the core issues and concepts, define the scope of the review, and identify appropriate resource materials (e.g., discovery requests, exemplar documents).

Project Management: The attorneys and review manager must put careful thought into the project timetable and into establishing the workflow to meet project goals. To this end, it is important to consider a number of factors, including the volume of data slated for review, established deadlines, and resources and staffing available to support the project. Attorneys should work with project managers to establish timelines sufficient to address the needs of the matter, as well as performance metrics and milestones to ensure the project is moving in the desired direction. It may be useful to establish deadlines for deliverables, require managers to provide regular status reports, as well as conduct periodic meetings or telephone conferences to assess progress.

Selection of Vendors and Technologies: At an early stage in the project, the attorneys should consult with knowledgeable internal or external resources to investigate vendors and technologies available to support the review project. In conducting this assessment, attorneys must consider the needs of the project and thoroughly vet prospective candidates and technology platforms to assess their capabilities and performance record.

Team Selection: The success of the review project will be inevitably linked to the team built to conduct the review and manage the process. When creating the team, it is important to evaluate the capabilities of the potential team members. As previously

discussed in the context of vendor selection, attorneys should evaluate the needs of the project in building the team (e.g., technical capabilities, experience with the subject matter, and cost factors). It may be appropriate to build a core legal team to oversee the vendor and review team, but this core legal team must have a firm grasp of the scope of the review, the applicable deadlines, and the sensitivities of the subject matter. It is important each member of the team is thoroughly briefed on the matter and knows their role in the project.

§ 8.11:4 Setup Review Room and Training the Team

Review Location: At an early stage, attorneys should assess the needs of the project and determine if an on-site review room is appropriate or if the project may be conducted at an off-site location (e.g., a vendor provided location). In any event, the review room must be evaluated to ensure it will support the hardware and software required for the review. Work with knowledgeable internal or external resources and coordinate with the vendors providing the review technology to ensure the site meets the requirements of the project. Ensure the review site is well-lit and free of distraction to create an environment conducive to an effective review.

Training and Reference Materials: The review team must have access to useful training and reference materials at the review site. In preparing the room for the review project, the core team should determine what materials must be readily available (electronically or physically) at the site to assist the review team and ensure an effective and efficient review. If client materials will be made available at the review site, the review team and project manager must ensure that proper safeguards are put into place so the material does not leave the secure environment of the site.

Training Presentation: Prior to initiating the actual review, the core team should meet with the review team and conduct a focused training session. At this training, provide the review team with the key information needed to complete the project, including (a) background of the matter, (b) scope of the review, (c) key legal and factual issues, (d) key custodians, (e) concise explanation of technical definitions and concepts, and (f) project deadlines. Likewise, discuss the mechanisms for questions to be submitted to the core team, as well as the opportunities for the review team and core team to discuss the review project.

§ 8.11:5 Conducting the Review

In advance of the review, collected ESI must be culled to narrow the review set to a more manageable, focused set of materials. After culling and filtering the materials, the review team is properly situated to initiate the review and identify the materials appropriate for production, as well as the privileged and confidential materials.

In a large document set it is advisable to first assess the volumes of material and project deadlines and then determine if there is a logical method to divide the review set to ensure deadlines are met. It may, for example, be appropriate to have materials from key custodians reviewed at the onset to identify documents and provide additional information to expand the understanding of key factual issues. Likewise, it may also be appropriate to identify key custodians or custodians with sensitive information and then have senior members of the review team review the material to ensure additional layers of scrutiny are applied to the document set.

§ 8.11:6 Status and Progress Reporting

Question and Answer Sessions: Once the review is underway, the core team should conduct sessions with the review team. The sessions are excellent opportunities for the review team to get feedback from the core team on their performance. More importantly, the sessions provide a forum for the review team to raise questions about the document sets. In so doing, the core team is able to gain an understanding of the issues being encountered by the review team and provide guidance on those issues to ensure consistent treatment of documents by the review team.

Reviewer Input Opportunities: The core team should establish opportunities for the review team to provide input to the core team on the core issues in the matter. In training the review team at the onset of the review, the core team is likely operating with limited information and without the benefit of in-depth review of the majority of relevant documents associated with the project. Likewise, it is also important for the review team to be able to report technical issues, error files, and other types of feedback to the core team to enhance the review project.

§ 8.11:7 Quality Control and Validation

Quality control and validation measures should be put into place to ensure the review is accurate and consistent. In most instances the review platform will provide the core team with the ability to conduct quality control reviews of document subsets reviewed by the review team. This feature allows the core team and project manager to identify common errors, poor-performing reviewers, or other issues that must be addressed as early as possible to avoid undercutting the effectiveness of the review. This type of quality control review may involve either a second-level review of all reviewed sets or their subsets. Discuss quality control measures with the project manager and vendor team before beginning the review to ensure a suitable system is in place.

§ 8.12 Conclusion

Neither the discovery rules nor the case law interpreting them have created any bright-line rules to define a "reasonable" search. Parties are not expected to identify every document, and responsive and relevant documents will be left behind by even diligent searches.⁴¹ While parties can estimate the recall and precision of their searches based on sampling, these raw numbers by themselves do not automatically determine if the search or culling process was reasonable, and there is certainly no magic threshold for recall or precision. Relevance and responsiveness are not binary concepts, and certain information and documents are more important than others. A search that finds 99 percent of all the relevant documents but is expected to miss numerous "smoking gun" documents is not likely to be considered reasonable. Likewise, a search that identifies a low number of interesting documents (e.g., less than 50 percent of the responsive documents) could still be a reasonable search if the remaining documents are highly cumulative or marginally relevant.

Moreover, in order to improve recall, searches almost always have to be broadened, which generally hurts precision. Thus the cost of conducting the review increases and, more importantly, the cost of identifying each responsive document goes up because more irrelevant documents must be manually reviewed. The question then becomes whether the benefit of the improved recall (i.e., the higher percentage of responsive documents identified) is worth the cost of reviewing additional irrelevant documents, or if it is reasonable to not broaden the search to capture more relevant documents since it will increase the cost of the review too much.

Finally, proper selection of the review team, developing a review strategy, and monitoring progress and quality are required.

^{41.} See Da Silva Moore, et. al. v. Publicis Groupe & MSL Group, 287 F.R.D. 182, 189 (S.D.N.Y. 2012).

Chapter 9

Format of Production

David J. Kessler and Sumera Khan¹

§ 9.1 Introduction

Electronically stored information ("ESI") exists and can be produced in various forms, which often becomes a particularly contentious issue in litigation. Rules adopted in the state of Texas as well as those implemented federally were designed to resolve these disputes, but all too often parties still bring these issues to the court for resolution.

Most of these disputes involve a tug-of-war regarding whether loose ESI files (like Word documents, PowerPoints, e-mails, and Excel spreadsheets) should be produced in "native" format or as some fixed image with appropriate searchable text and metadata (such as TIFF+, which is a combination of static images, extracted text files, and metadata, and sometimes includes added content like the names of attributable custodians and Bates control numbers). While Federal Rule of Civil Procedure 34 does not explicitly require responding parties to produce documents in their native format, some requesting parties argue that any other format is not "reasonably useable." The Texas state rules require that a requesting party specify the form in which it wants documents produced, and outside of objections by the responding party, that form is generally upheld.

Neither the Texas Rules of Civil Procedure nor the Federal Rules of Civil Procedure require that ESI be produced in a certain format, though both sets of rules have a procedure for requesting format and, more specifically, federal rules have explicit default formats. This chapter will briefly lay out the issue, the law, the choices, and the aspects that should be taken into consideration regarding whether to require a native production.

^{1.} This chapter builds off of work done by David Kessler and Dan Regard in their chapter on Format of Production in Electronic Discovery Institute's *Federal Judges' Guide to E-Discovery 2.0*. The authors thank the Electronic Discovery Institute and Dan Regard.

§ 9.2 Texas Rule of Civil Procedure 196.4

Notably, Texas was one of the first jurisdictions to recognize that many relevant documents exist electronically and are discoverable. This point was codified in 1999 in Tex. R. Civ. P. 196.4, Electronic or Magnetic Media, which provides the following guidance:

To obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced. The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If the responding party cannot—through reasonable efforts—retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules. If the court orders the responding party to comply with the request, the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.

Tex. R. Civ. P. 196.4 (emphases added). While the Texas rules explicitly require the requesting party to specifically request the electronic data it wishes to receive, rule 196.4 does not explicitly state how the responding party is required to adhere to the format request, nor does it address how courts are supposed to weigh the requested format versus the format that a responding party wants to use.

§ 9.2:1 Defining a Procedure for Requests for ESI

Although the notes and comments to the rule provided some guidance,² ten years later, the Texas Supreme Court in *In re Weekley Homes, L.P.,* 295 S.W.3d 309 (Tex. 2009) and then more recently in *In re State Farm Lloyds,* 520 S.W.3d 595 (Tex. 2017) addressed Tex. R. Civ. P. 196.4 more directly and suggested a protocol that parties may follow when making requests for ESI, including requirements related to the format of production.

^{2. &}quot;A party requesting production of magnetic or electronic data must specifically request the data, specify the form in which it wants the data produced, and specify any extraordinary steps for retrieval and translation. Unless ordered otherwise, the responding party need only produce the data reasonably available in the ordinary course of business in reasonably usable form." Tex. R. Civ. P. 196.4 1999 advisory committee notes and comments.

Format of Production

at 606⁴

For example, a party should specifically request the production of files located on backup tapes rather than relying on a request for "all electronic documents" to cover these types of files. Tex. R. Civ. P. 196 4.³ The Texas Supreme Court has now clarified that a request for a certain format of production does not mean that the responding party must automatically comply because "neither the requesting nor the producing party has a unilateral right to specify the format of discovery." *In re State Farm Lloyds*, 520 S.W.3d at 604. The responding party must then produce any electronic information that is "responsive to the request and is reasonably available to the responding party in its ordinary course of business." *In re State Farm Lloyds*, 520 S.W.3d at 606. If "the responding party cannot—through reasonable efforts—retrieve the data or information requested or produce it in the form requested," the responding

party must specifically object on those grounds. In re State Farm Lloyds, 520 S.W.3d

To the extent the parties cannot resolve the dispute, either party may request a hearing on its objection to the discovery request. At the hearing, the responding party must demonstrate that the requested information or format is not reasonably available because of undue burden or cost. In re Weekley Homes, 295 S.W.3d at 315. When a reasonably useable form is readily available in the ordinary course of business, the trial court must assess whether any enhanced burden or expense associated with the requested form is justified when weighed against the proportional needs of the case. The Texas Supreme Court weighed in on the proportionality inquiry, stating that it requires a case-by-case balancing to weigh any burden or expense of producing data in the requested form against the relative benefits of doing so, the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the requested format in resolving the issues. In re State Farm Lloyds, 520 S.W.3d at 608. The court also stated that "if these factors preponderate against production in the requested form, the trial court may order production as requested only if the requesting party shows a particularized need for data in that form and 'the requesting party pay[s] the reasonable expenses of any extraordi-

^{3.} See, e.g., In re Methodist Primary Care Group, 553 S.W.3d 709 (Tex. App.—Houston [14th Dist.] 2018, no pet.) (finding that although a party seeking discovery of electronic data did not reference Tex. R. Civ. P. 196.4 in its requests for production, it sufficiently invoked the rule by making clear it sought electronic data, and the responding parties thus had a duty to undertake reasonable efforts to produce responsive and reasonably available electronic data); *In re Jordan*, 364 S.W.3d 425, 426 (Tex. App.—Dallas 2012, orig. proceeding) (holding that written requests merely asking for computer hard drives are insufficient under rule 196.4).

^{4.} See, e.g., In re Shipman, 540 S.W.3d 562, 566–67 (Tex. 2018) (finding that because the producing party maintained a position that all responsive documents in his possession had been produced already, he could not lodge a rule 196.4 objection without contradicting his position).

nary steps required to retrieve and produce the information." *In re State Farm Lloyds*, 520 S.W.3d at 600 (citation omitted).

§ 9.2:2 Specific Requests for ESI

The specificity requirement of Tex. R. Civ. P. 196.4 is designed "to ensure that requests for electronic information are clearly understood and disputes avoided." *In re Weekley Homes*, 295 S.W.3d at 314. Nevertheless, Texas courts have found that a request for documents in "reasonably useable" or a "reasonable manner" are sufficient.

By way of example, in In re Waste Management of Texas, Inc., 392 S.W.3d 861 (Tex. App.—Texarkana 2013) the court considered whether a responding party was entitled to mandamus relief with respect to a court order that required the party to produce data similar to what it had produced earlier (in PDF⁵ form without metadata) in "native" format. In re Waste Management of Texas, Inc., 392 S.W.3d at 865. The appellate court found that, given the procedural posture of the case, the responding party was not entitled to mandamus relief because the difference of \$3,000 between the cost of producing metadata in PDF form and the trial court's order was not significant. In re Waste Management of Texas, Inc., 392 S.W.3d at 876. As part of this analysis, the court examined the requesting party's request for production of documents in a "reasonable manner." In re Waste Management of Texas, Inc., 392 S.W.3d at 874. The court found this sufficient under the rules and determined that such a request was the functional equivalent of the federal "reasonably useable form or forms." In re Waste Management of Texas, Inc., 392 S.W.3d at 874. As such, the requesting party had not waived its right to production of documents in a form different than what the responding party produced. In re Waste Management of Texas, Inc., 392 S.W.3d at 876. Importantly, the Waste Management court never examined the trial court's decision to require native production or if the PDF format was "reasonably useable" or if another production format would be more reasonably useable.

§ 9.2:3 Responding to Specific ESI Formats

The Texas Supreme Court has made it clear that unless a court orders otherwise, "the responding party need only produce the data reasonably available in the ordinary

^{5.} Portable Document Format (PDF): A file format technology developed by Adobe Inc. to facilitate the exchange of documents between platforms, regardless of originating application, by preserving the format and content. *The Sedona Conference Glossary: E-Discovery & Digital Information Management (Fourth Edition)*, 15 Sedona Conf. J. 305 (2014).

Format of Production

course of business in reasonably useable form." In re State Farm Lloyds, 520 S.W.3d at 600. In that case, residential homeowners brought suit against their insurer, State Farm, and other entities in Texas state court for alleged underpayment related to hail damage claims. At the homeowners' request, the trial court ordered that all ESI be produced in native or near-native form (such as XLS for Excel spreadsheets) rather than a searchable but static form (such as PDF) that State Farm proposed. The homeowners argued that native production would allow them access to useable metadata that would not otherwise be available in static form, such as formulas in Excel spreadsheets. Their expert further opined that production of ESI in static form would be more expensive for the homeowners due to the fact that storage costs rise with the size of the file. Comparatively, the burden on State Farm to produce in native format would be minimal, if any. State Farm, on the other hand, stated that it processes more than 350,000 new claims a day and that the claims are routinely converted into static format and maintained in an enterprise claims database. Without quantifying time or expense, State Farm argued that to produce information in native form would require State Farm to create a new process that would depart significantly from their standard business procedures. The Texas Supreme Court remanded the case and advised that the trial judge should reweigh the State Farm discovery dispute in light of its new guidance on proportionality. The court said that "litigants achieve a 'just, fair, equitable and impartial adjudication . . . with as great expedition and dispatch and at the least expense . . . as may be practicable." In re State Farm Lloyds, 520 S.W.3d at 615 (citing Tex. R. Civ. P. 1).

The Texas Supreme Court's decision confirms that all discovery, whether electronic or otherwise, must be appropriate and proportional in each case, which extends to the format of production:

Under our discovery rules, neither party may dictate the form of electronic discovery. The requesting party must specify the desired form of production, but all discovery is subject to the proportionality overlay embedded in our discovery rules and inherent in the reasonableness standard to which our electronic-discovery rule is tethered. The taproot of this discovery dispute is whether production in native format is reasonable given the circumstances of this case. Reasonableness and its bedfellow, proportionality, require a case-by-case balancing of jurisprudential considerations, which is informed by factors the discovery rules identify as limiting the scope of discovery and geared toward the ultimate objective of "obtain[ing] a just, fair, equitable and impartial adjudication" for the litigants "with as great expedition and dispatch at the least expense ... as may be practicable.

In re State Farm Lloyds, 520 S.W.3d at 599.6

§ 9.2:4 Permitting Inspection of ESI vs. Production

Tex. R. Civ. P. 196.2 requires that a response to a request for documents "state, as appropriate, that ... production, inspection, or other requested action will be permitted as requested "By practice, it is in the responding parties' discretion to choose whether to allow inspection or to produce the responsive documents. See, e.g., Steenbergen v. Ford Motor Co., 814 S.W.2d 755 (Tex. App.-Dallas 1991, writ denied) (permitting the responding party to make available its document production in a reading room at its corporate headquarters where opposing counsel could inspect and photocopy documents because the production exceeded 100,000 documents). Generally, like in federal court, Texas state courts only interfere with a responding party's discretion if production is infeasible or if the responding party has shown that it cannot or will not properly produce the documents. Overall v. S.W. Bell Yellow Pages, Inc., 869 S.W.2d 629, 631 (Tex. App.—Houston [14th Dist.] 1994, no writ) (finding that a party who responded to a request for production by stating that the three-document production was available for inspection at its attorney's office was not a valid response because there was no justification or burden in producing photocopies of the production).

§ 9.2:5 Organization of Production

Tex. R. Civ. P. 196.3(c) provides that "[t]he responding party must either produce documents and tangible things as they are kept in the usual course of business or organize and label them to correspond with the categories in the request." This requirement is a separate consideration than the format of ESI production.

A responding party may choose to produce documents as they are kept in the usual course or may organize them by categories under the requests for production. *Tex. Gen. Land Office v. Porretto*, 369 S.W.3d 276, 290 (Tex. App.—Houston [1st Dist.] 2011, pet. denied) ("a trial court cannot sanction a party for failing to organize responsive material according to the method its opponent prefers when the discovery response complies with an alternate method permitted under the rules"); *see also In re*

^{6.} The court further recognized that given this application of proportionality, the Texas rules now align with the electronic discovery practice under the federal rules, whose plain language does not permit either party to dictate the form of production for ESI. *In re State Farm Lloyds*, 520 S.W.3d at 655, n.7 (citing *In re Weekley Homes*, 295 S.W.3d at 309, 316–17). Texas courts may therefore be guided by federal court decisions addressing what is reasonably available in terms of production format.

Format of Production

Colonial Pipeline Co., 968 S.W.2d 938, 941 (Tex. 1998) (orig. proceeding) (holding that trial court abused its discretion in ordering party to produce inventory in response to request for production); *McKinney v. Nat'l Union Fire Ins. Co.*, 772 S.W.2d 72, 73 n. 2 (Tex. 1989) (declaring that rule governing requests for production "cannot be used to force a party to make lists or reduce information to tangible form").

§ 9.2:6 Production of Metadata

Metadata is described as "data about data" and is often requested to be produced in most litigation. However, the high court in Texas has clarified that "production in a metadata-friendly format is [not] necessarily required." *In re State Farm Lloyds*, 520 S.W.3d 595, 605 (Tex. 2017). One of the reasons the homeowners in that case requested native format was to get access to metadata. However, the court explained that "metadata serves no genuinely useful purpose in many cases" and may be necessary "to the litigation when the who, what, where, when, and why ESI was generated is an actual issue in the case . . ." (such as in a wrongful termination case). *In re State Farm Lloyds*, 520 S.W.3d at 608, 609. Except for where there is a specific need for information, given the claims and defenses in the case, the Texas Supreme Court appears to suggest that production of metadata should not be necessary. However, there may be other reasons why a party may request metadata, such as identifying the authors of documents in a complex litigation or confirming the document creation date where that information may not be readily available on the face of the document.

While not addressed squarely by the Court in *In re State Farm Lloyds*, certain metadata (like author, date created, senders and recipients) can be helpful in documentintensive cases to enable the requesting party to search and sort the documents produced to reasonably identify the documents it wants to use in depositions, motions, and hearings.

§ 9.3 Federal Rule of Civil Procedure 34

In format of production disputes, the pertinent portion of the federal rules is as follows:

- (a) Procedure
- (1) Contents of the Request. The request:
 - (A) must describe with reasonable particularity each item or category of items to be inspected;

- (B) must specify a reasonable time, place, and manner for the inspection and for performing the related acts; and
- (C) may specify the form or forms in which electronically stored information is to be produced.
- (2) Responses and Objections.
 - (A) Time to Respond. The party to whom the request is directed must respond in writing within 30 days after being served or—if the request was delivered under rule 26(d)(2)—within 30 days after the parties' first rule 26(f) conference. A shorter or longer time may be stipulated to under rule 29 or be ordered by the court.
 - (B) Responding to Each Item. For each item or category, the response must either state that inspection and related activities will be permitted as requested or state with specificity the grounds for objecting to the request, including the reasons. The responding party may state that it will produce copies of documents or of electronically stored information instead of permitting inspection. The production must then be completed no later than the time for inspection specified in the request or another reasonable time specified in the response.
 - (C) Objections. An objection must state whether any responsive materials are being withheld on the basis of that objection. An objection to part of a request must specify the part and permit inspection of the rest.
 - (D) Responding to a Request for Production of Electronically Stored Information. The response may state an objection to a requested form for producing electronically stored information. If the responding party objects to a requested form—or if no form was specified in the request—the party must state the form or forms it intends to use.
 - (E) Producing the Documents or Electronically Stored Information. Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:

- (i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;
- (ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and
- (iii) A party need not produce the same electronically stored information in more than one form.

Fed. R. Civ. P. 34(b).

§ 9.3:1 Inspections vs. Production

Fed. R. Civ. P. 34(b)(2)(B) makes it clear that a responding party can choose between producing copies of documents and ESI, or allowing the requesting party to inspect the information at the responding party's premises. Unless a responding party cannot reasonably produce the information or fails to do so, the choice of producing documents instead of allowing inspection should be respected. The format of production only matters if the responding party chooses to produce copies of ESI instead cf allowing inspection.

§ 9.3:2 Determining Organization of Production

Fed. R. Civ. P. 34(b)(2)(E)(i) relates to the organization of production, which is distinct from the format of production that is addressed in Fed. R. Civ. P. 34(b)(2)(E)(ii). The phrase that a responding party "must produce documents as they are kept in the usual course of business" under rule 34(b)(2)(E)(i) should not be conflated with the phrase under rule 34(b)(2)(E)(ii) that a party "must produce it in a form or forms in which it is ordinarily maintained."⁷ Under this rule, a responding party has the discre-

^{7.} At least one court has found that rule 34(b)(2)(E)(i) does not apply to ESI and thus producing parties do not need to produce ESI either as it is ordinarily maintained or by document request. Anderson Living Trust v. WPX Energy Prod., LLC, 298 F.R.D. 514, 527 (D.N.M. 2014). Other courts have found that rule 34(b)(2)(E)(i) does apply to ESI. See, e.g., McKinney/Pearl Rest. Partners, L.P. v. Metro. Life Ins. Co., 322 F.R.D. 235, 253 (N.D. Tex. 2016); Chet Morrison Contractors, Inc. v. Medco Energi US LLC, No. 08-1638, 2009 WL 2762049 at * 2 (E.D. La. Aug. 25, 2009); Valeo Elec. Sys., Inc. v. Cleveland Die & Mfg. Co., No. 08-cv-12486, 2009 WL 1803216, at *2 (E.D. Mich. June 17, 2009).

tion to produce the documents as they are organized in the ordinary course or to produce them by document request. This choice should not be overruled unless the responding party fails to comply with its choice.⁸ Generally, a responding party produces e-mails in the usual course when it provides sufficient information about the email, typically including the custodian for the e-mail, information to link e-mails with attachments, and the date and time the e-mail was sent or received. For non-email loose ESI, a responding party should provide the custodian and the file path.

§ 9.3:3 Determining Format of Production

Under Fed. R. Civ. P. 34(b)(1)(C), the requesting party may identify the format for each document produced, including different formats for different types of documents. The responding party is allowed to object to such a request under rule 34(b)(2)(D). If the responding party objects or if the requesting party does not state a particular format in its requests, the responding party must state the format (or formats) in which it intends to produce ESI. If the parties cannot agree on a format and the court needs to select one, then "the court is not limited to the forms initially chosen by the requesting party, stated by the responding party, or specified in this rule for situations in which there is no court order or party agreement." *See* Fed. R. Civ. P. 34 2006 advisory committee notes.

§ 9.3:4 Baseline for Formats: Native and Reasonably Useable

Fed. R. Civ. P. 34(b)(2)(E)(ii) and 34(b)(2)(E)(iii) set the parameters of what formats can be produced by the responding party. Absent some agreement between the parties, the responding party cannot be *forced* to produce ESI beyond the native format in which it is maintained in the ordinary course of business (though this can be a dangerous shortcut). At the same time, the responding party cannot choose to produce ESI in a format that is both not how it is maintained in the ordinary course of business *and* not reasonably useable.

Generally speaking, this means that the responding party is free to produce its ESI in any reasonable format and does not have to produce the documents in the form in which they are ordinarily maintained. *See* Fed. R. Civ. P. 34 2006 advisory committee notes. Moreover, a responding party generally does not have to produce the same documents in more than one format. *See* Fed. R. Civ. P. 34(b)(2)(E)(iii); *see also* Fed. R.

^{8.} See, e.g., CooperVision, Inc. v. Ciba Vision Corp., No. 2:06-CV-149, 2007 WL 2264848, at *5 (E.D. Tex. Aug. 6, 2007) ("simply placing documents in boxes and making them available does not conform to [federal r]ule [34].").

Civ. P. 34(b)(2)(C)(i) ("On motion or on its own, the court must limit the frequency cr extent of discovery otherwise allowed by these rules or by local rule if it determines that . . . **the discovery sought is unreasonably cumulative or duplicative**" (emphasis added)).

§ 9.3:5 Reasonably Useable

The phrase "reasonably useable" is not defined in the federal rules, and the 2006 advisory committee notes only say—

[T]he option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature.

Fed. R. Civ. P. 34 2006 advisory committee notes (emphasis added). Given this comment, it is clear that the searchability of the production format is one key feature to determine whether it is reasonably useable. However, beyond searchability, the focus of "reasonably useable" is a practical one: how will the ESI be used in the litigation? In most cases, ESI is searched and reviewed to identify key documents that are then shown to witnesses, opponents, and the court to present facts and to advocate positions. This is why the advisory committee considered searchability so important—to allow the requesting party to find documents in the large volumes produced. On the other hand, if the documents need to be used for other purposes in the litigation, those needs can impact the format in which documents should be produced. Because there are costs to the responding party for different formats, both direct and indirect, the marginal value of different formats needs to be balanced with the additional costs.

"Reasonably useable" does not mean reasonably equivalent or that the parties have parity in their use of produced documents. *In re Benicar (Olmesartin) Products Liability Litigation*, No. 15-2606 (RBK-JS), 2016 WL 5817262, at 11 (D.N.J. June 30, 2015) (oral op.), ("[P]laintiffs repeatedly argue that plaintiffs should have parity with defendants. This argument is not compelling. The federal rules only require that defendants produce their ESI in a reasonably usable format."). Moreover, the requesting party cannot demand production in one format versus another just because one would allegedly ease a party's review process. *See U.S. ex rel. Carter v. Bridgepoint* *Educ., Inc.*, 305 F.R.D. 225 (S.D. Cal. 2015). This evaluation is case-specific, and courts are "tasked with evaluating the necessity of the information requested by Plaintiffs against the burden on Defendants of producing the information in the requested format." *Dizdar v. State Farm Lloyds*, 2015 U.S. Dist. LEXIS 186873, at *34–35 (S.D. Tex. Jan. 7, 2015) (finding that any burden incurred by the responding party in producing information in "native" or "near native" format is too much, and granting the responding party's request to produce ESI in the searchable static image files routinely prepared for litigation).

§ 9.4 Formats of Production—Loose Files

Most ESI produced in litigation consists of e-mail (e.g., Outlook messages) and loose, stand-alone documents like word processing files (e.g., Word), presentations (e.g., PowerPoint), or spreadsheets (e.g., Excel). For these files, the biggest production format conflict between parties is whether they should be produced in native or TIFF+ format (which is described in more detail below, but is essentially a static image of the file with extracted text and metadata to make it searchable).

§ 9.4:1 Native Format

As discussed above, the phrase "native format" does not appear in either the Texas state or federal rules. Rather, it is the "form or forms in which [ESI] is ordinarily maintained." Practically speaking, most parties use the phrase "native format" to mean an unaltered, default format of how information is kept in the normal course of business. *See The Sedona Conference Glossary: E-Discovery & Digital Information Management* (4th ed. Apr. 2014) ("Native Format: Electronic documents have an associated file structure defined by the original creating application. This file structure is referred to as the native format of the document.").

For individual loose ESI, such as Microsoft Office files, the native format appears easy to define, typically with a one-to-one correspondence between an individual file and what is intended to be produced (redactions notwithstanding). However, even for these files there is some ambiguity because many companies may create a file in one format and store it another. For example, a party may create a memo in Word format and archive it in PDF format (with or without embedded text to make it searchable) so that it cannot be edited. At most, native should mean how the company maintained the document as of the date of preservation, not how it was created or how any third party may have created, stored, or transmitted it.
litigation can be stored in multipl

§ 9.4

E-mails, perhaps the most common form of ESI in litigation, can be stored in multiple locations, and the native format could represent a mailbox, a MSG, an EML, an OST, a PST, or a variety of other formats all supported by e-mail systems or reflective of the actual file format of the e-mail as it moves from one location and application to another. This is because e-mails usually start as, and end up as, complex hybrid records stored in complex relational databases.⁹

As ESI file format becomes more individualized and dynamic, and as its metadata becomes more extensive and more dispersed throughout the computer system, the burden of preserving integrity, collection, management, review, redaction, production, and practical usage within a litigation context becomes exponentially greater. Computers create and store information in a manner that is convenient for the computer, the application, or the "user experience," not necessarily for future use in litigation.

Two arguments for native production are based on misconceptions of how e-discovery technology works. First, some have argued that the newest data analytic software and technology-assisted review (TAR) tools need native production, or at least they will work better with native files. The argument is that native files contain more information and therefore help the tools and software work. This is incorrect; except for forensic technology (which is rarely used on productions), none of this technology operates on native formats. In fact, when provided with native files, the technology actually will extract the text and metadata needed—exactly like TIFF+ productions. Similarly, some have argued that native productions are more searchable (based on the same theory: that more information makes it more searchable). This is not accurate because to build an index to search across files, the discovery technology, again, needs to extract the text out the files. Thus, native production is no more searchable than TIFF+ and, in fact, TIFF+ is more searchable than the files as they exist in the ordinary course of business because they can be easily searched across file types.

§ 9.4:2 TIFF+

Over the last twenty years, law firms and litigation support firms have developed technologies to manage paper and, increasingly, ESI through the conversion of files to a static image as a Tagged Image Format File (TIFF). When these images are augmented with logistical information, fielded information (metadata), and full-text

^{9.} For other database records, which can be less complicated or more complicated than e-mails, the challenges can be greater simply because most litigants have less familiarity with these databases than they do with an e-mail system. These are ciscussed in more detail below.

extraction files, this collection is referred to as a TIFF+ production. Each of these component parts is discussed below.

Because of the sheer number of years and cases that TIFF+ has been used, virtually all e-discovery tools (old, current, and emerging) accommodate, if not prefer, TIFF+ productions. Therefore, when faced with a situation where parties fail to agree, the most common ground continues to be TIFF+ format. Moreover, when the primary use by the requesting party is to find and read a document and then potentially use it as an exhibit as evidence in a deposition, motion, or hearing, then TIFF+ is as useful, if not more useful, then native production. That being said, because of one-off ad hoc concerns about individual documents, requesting parties should be able to obtain native production of specific documents. These exceptions, however, should not swallow the general proposition.¹⁰

Static Image, or TIFF: The conversion of the native file to a static image, or TIFF, creates a frozen picture of each page of the document. This normalizes the evidence and ensures that everyone who uses and sees the document in the litigation sees it the same way. Because this freezes the document, it is important that any relevant hidden or embedded data¹¹ is exposed so that everyone can see them throughout the litigation. By creating the TIFF image,¹² the document is not only much more difficult to edit, but it can be branded with Bates labels, which makes identifying unique pages easier, and confidentiality designations, which are crucial from a data security perspective.

Moreover, static images (as opposed to native files) can be redacted, which is crucial for withholding privileged information. Also, given the rise of more and more privacy and data protection laws in the U.S. and abroad, redaction is important for protecting the personal data of third parties, employees, consumers, and vendors. Finally, given

^{10.} For a countervailing position on why a native file form of production is advisable under certain circumstances, see Craig Ball, *The Case for Native Production*, Practice Law Journal, p. 32 (Oct./Nov. 2014), www.craigball.com/LIT_OctNov2014_EDiscoveryBulletin.pdf.

^{11.} Many ESI formats allow for both hidden and embedded data. Hidden data is information within the ESI that the user can view or not view depending on filters within the application (e.g., comments, redlines on Word processing files, or speaker notes in presentation files). Embedded data is information—or even whole additional files—that is included in the content of ESI that may not be easily viewable by results in viewable information (e.g., spreadsheets in presentations or formulas in spreadsheets). Because hidden and embedded data can come in many forms and presented in many different ways, it is generally most fair to programmatically expose this information so that all reviewers and witnesses can review it equally.

^{12.} The static image does not need to be TIFF. It can be PDF or other images, but TIFF is the most common. Because TIFF does not render in color, many parties use JPEGs for documents whose color is important to their meaning. Because JPEGs are much, much larger than TIFFs, parties prefer not to use them for run-of-the-mill black-and-white documents.

Format of Production

the increased sensitivity to data breaches and requesting parties being targeted as a vulnerable trove of valuable data, redactions will become more common and necessary to protect irrelevant but commercially sensitive data.

Extracted Text: Extracted text is one half of the "plus" in TIFF+ and is what makes the content of documents searchable when producing in this format. Modern processing software can extract virtually all text, both revealed and hidden, in a systematic way from a native file and create a text file that can be linked to its TIFF images. This allows a requesting party to apply search terms, conduct concept analytics, and apply other TAR, such as predictive coding, regardless of original format.

Metadata: Metadata load files are most of the second half of the "plus" in TIFF+. These load files not only allow searching and TAR across the documents, but, as fielded data, load files make it easy to sort and filter (e.g., all e-mails sent by Steve Smith). Though metadata is often called the "data about data," this vague description does not help determine what it is, when it should be produced, and if it requires native production.

Most ESI contains information (or has information associated with it) that is useful in using, searching, and identifying the document that may not be contained within the content of the file or, if it is, extracting the content into a separate data field that makes the information more useful. For example, filename and author fields are not contained within the body of much ESI, but these tend to have relevant information (e.g., the filename "XYZContract v2 1-1-12" could tell a party that someone believed this document was the second version of the contract and put the date January 1, 2012, on it). On the other hand, the recipients and subject lines of an e-mail are contained within its content, so extracting them makes them easier to search, and they can be filtered or sorted in alphanumeric order.

Metadata is often created automatically by a computer or IT system, but it can also be created by the user. Examples include "date created" metadata, which is populated by the IT system, and the subject line of an e-mail, which is created by the sender. Like all ESI, the mere fact that a metadata field contains information does not mean that the information is accurate or true. Consider document author metadata. This is autopopulated by the system based on who is the owner of the software license or who is logged into the computer, but that may not be the person who actually wrote the document.

To be effectively used, metadata needs to be extracted from the document. As such, even if native productions are made, the metadata they contain cannot effectively be

used until it is pulled and placed in load files that are identical to what is produced in TIFF+ format.

Metadata is different for every type of file format; many files have hundreds of potential pieces of metadata. The table at the end of this chapter shows a list of metadata that is typically exchanged and is generally considered to make TIFF+ reasonably useable. In specific matters, more or less metadata may be necessary depending on the needs of the case and what the responding party needs to do with the production.

The "load file" portion of "metadata load file" also acknowledges that a metadata file often contains generated information specific to the collection and production process that may not exist in the original native data, such as the starting and ending Bates numbers for a given document, the starting and ending Bates numbers for a family of documents, and the custodian source.

§ 9.4:3 Native+

One of the most common dangers of using the word "native" is that it can be abused if defined to mean something more than how a file was kept in the ordinary course of business. A request for native files with extracted text files and certain extracted metadata in a load file is not a request for native production because in the ordinary course of business a party does not store extracted text and metadata in a load file. As explained above for TIFF+ format, the extracted text file and the metadata load file are artifacts of discovery processing that allow the static image to be searchable across its content and key metadata. Requesting parties typically want these processing artifacts because native files are not as easy to use without them and the requesting parties do not want to spend the money to process the files themselves. However, under the parameters of Fed. R. Civ. P. 34(b)(2)(E)(ii), this request is not within the ordinary course of how a document would be kept and is therefore beyond the scope of what responding parties can be compelled to provide. Most Native+ requests masquerade as requests for native format production since both parties will shortcut to that phrase inadvertently or intentionally.

§ 9.5 Hidden Costs of Native Production

To understand why certain responding parties resist the production of native format across their entire production of loose ESI, it is important to understand the cost of native production and the costs of native format to the overall discovery and to the case.

Format of Production

Expense: It is often stated that producing in native format is cheaper than producing in TIFF format. While it is true that native production avoids the cost of formatting to TIFF, this is usually less than three cents per page and is a de minimis amount when compared to the cost of processing and reviewing the files. Given other costs of native

production detailed below, it is not cheaper. Almost all software designed for hosting and reviewing documents in litigation can process TIFF+ productions at little to no cost. On the other hand, a true native production needs to be processed to extract text and metadata to make it searchable.

Review of native files can also be very time consuming. While one could theoretically review each native file in its native application, this method is practically impossible because of the burden of not only needing every application, but also because of the time it would require to open and access each application and document. Therefore, one must question whether a native file requester truly intends to review each and every file in a native application. In other words, what is the real intent behind the request for native?

In most cases, native review would sc greatly increase the time of the review that it would render most discovery schedules nearly impossible to comply with. Moreover, reviewing in this fashion, even for small matters, runs the risk of inadvertently altering the produced document and therefore destroying the integrity of the evidence. Impracticalities only cascade from there; for instance, how are documents to be used in depositions? In hearings? In motions? At trial? How do the parties grapple with real authentication concerns? Why invite accusations of alteration? While static images are possible to edit, it is impossible to do so accidentally, and it takes incredible skill to do so in a way that is not easily detected by the naked eye. This problem leads to two other great costs of native productions.

Data Security Issues: Because native files are so easily editable, producing native documents is a significant data security concern for producing parties. In essence, once native files are presented to requesting parties, they are then vulnerable to inadvertent or purposeful tampering. A single added space in the text will change the MD5 hash of the native file, making it impossible to trace for forensic authentication. As discussed above, native files cannot be Bates labeled or designated as confidential on a page level, which means the filename is the only designatable part, and filenames are easily changed. This means it can be very difficult to establish where a document was leaked and actually enforce any protective order. Given that many cases involve valuable, confidential, and private information, the security risk of native files is a significant and real concern for producing parties.

Evidentiary Concerns: Each application, computer, and printer treat native documents slightly different, therefore the native evidence can inadvertently (or intentionally) look different to different witnesses, parties, and to the court. Many lawyers and parties print out ESI to use in depositions or motions, but different printers (or even the same printers with different settings) will change pagination. Depending on how spreadsheet software is configured, the order in which columns and rows will print can differ. Moreover, depending on how the lawyer configures his or her software, whole portions of a file may not be visible (e.g., speaker notes in presentations or hidden columns in Excel). Except for very good reason, evidence should be normalized so that everyone can agree on what the evidence is. Imagine a scenario where the same document looks different in each party's 30(b)(6) deposition, and then is different again as a trial exhibit.¹³

In short, normalization removes the logistical chaos otherwise introduced in the entire discovery phase of litigation via unlabeled exhibits with variable formatting and pagination. Disorganization, battles of imprecision, and loss of time in depositions and hearing are all avoided by the use of TIFF+.

Authentication Issues: The ability to easily edit native files can lead to significant issues when authenticating documents in depositions. Understandably, parties do not want their witnesses testifying about files that may have been inadvertently or intentionally altered by their opponents.

Given the size and complexity of many files, a careful manual inspection of the files is not practically possible during the deposition, so the parties are faced with equally unattractive options of authenticating before, during, or after the deposition via MD5 hash. However, comparing MD5 hash values is not practical during the deposition due to time constraints. At the same time, the party taking the deposition typically does not want to tip its hand as to what documents it is going to show the witness, and comparing the values afterwards can cause testimony problems when the hash values do not match. This leads to complex deposition processes to validate exhibits that increase time and cost.

Moreover, in large productions of pure native documents, it can be hard to establish that documents used in motions or depositions were even produced, particularly if

^{13.} Of course, this assumes that it is possible for you (or the circuit court) to accept the native version of a document as evidence and include it in the record. There are potential problems, especially in state courts, if a native file cannot be kept in the record of the proceeding all the way through an appeal. Given the limited number of documents that are produced in cases that are actually presented as trial exhibits, these issues can be handled by the court on a one-off basis.

non-native documents (e.g., printouts) are used. Without the ability to search hash values, it may be hard to find the original document in the production, especially if the document has little or no searchable text.

§ 9.6 When TIFF+ Production Is Not Reasonably Useable

Experience has shown that the vast majority of productions can be facilitated with a static image of the document and a handful of common metadata fields, especially when the parties provide for the production on an as-needed basis of (a) dynamic "native" or alternative format copies. or (b) more extensive metadata. There have been litigations where the correct and full understanding of the entire life cycle of a handful of documents is central to the issues in the case. In these instances, metadata, forensic images, expansive discovery, and third party subpoenas have been appropriate. But again, this accounts for a small percentage of cases. Most cases require nothing more than TIFF+, and those that require more typically only require more for a handful of documents.

Despite all of these potential issues, there are limited instances where native production may be appropriate for specific reasons. That is, the following should be the exception, not the rule:

- Where the value of the ESI is not in text, like a voice mail or security video, and TIFF+ will not produce the relevant information
- Where the value of the ESI is dynamic and cannot be frozen (like a specific PowerPoint that contains animation)
- To show the authenticity of a specific e-mail or other specific ESI
- To reasonably use (e.g., to sort by column or row as an expert may need) certain types of documents (e.g., Excel files)
- To provide a reasonably useable format to a requesting party when a responding party has, after several attempts, failed to produce information as agreed to or in a reasonably useable format

§ 9.7 The Tricky Thing about Databases

Databases can be, but do not have to be, more complex and difficult than stand-alone, loose ESI.¹⁴ When the information from databases is going to be treated as a series of individual reports or documents (like invoices, contracts, or adverse event reports) for

review and presentation to witnesses, then such database information is comparable to, and is generally reasonably useable as, static images in TIFF+ format.

Alternatively, for tabular extractions that need to be analyzed, sorted, or tested by witnesses and experts, either spreadsheets or a delimited flat file (e.g., a comma-separated values file, or CSV) would be the most reasonable format for production. This allows import into generic database management tools for further analysis. Often, such productions also contain "header" information, which label the columns of data for the benefit of the receiving party.

However, it is rarely practical (or reasonable) to provide most databases in native format since these systems are highly complex, proprietary, and customized, and the requesting party would not be able to operate or view the database information without the underlying database management tools, software licenses, and institutional knowledge required to navigate such systems. It is also usually the case with most databases (as with most mailboxes or most computer hard drives) that while some of the data, or even most of the data, is responsive to data requests, typically all of the data is not. Producing databases in native format treats the entire container as responsive, as opposed to limiting production to that data that truly is responsive. The challenges of redacting a database in native format are also a subject of much delay and expense.

^{14.} For a more thorough discussion of databases and structured information, please review The Sedona Conference, *Database Principles: Addressing the Preservation & Production of Databases & Database Information in Civil Litigation*, 15 Sedona Conf. J. 171 (Sept. 2014), https:// thesedonaconference.org/sites/default/files/publications/171-216%20Database%20Principles_0.pdf.

Field Name	Description
Begin Bates	Beginning Bates number
End Bates	Ending Bates number
Begin/End Attachment	Bates range of full family
Att Count	Number of attachments to an e-mail
Parent/Child ID	Bates number of either the attachment (if parent e-mail) or parent e-mail (if attachment)
Custodian/Source	Name of the custodian or source of the document produced
Confidentiality	A document's confidential designation should be included in a field value as well as burned onto the images

Table:	Metadata	List
I auto	mulaua	LISU

Field Name	E-Mail or Non-E-Mail	Description
Subject/Title	E-mail	Subject/Re: Line of the e- mail
File Name	Non-e-mail	Name of the application file or attachment
Date and Time Sent	E-mail	E-mail sent date and time
Date and Time Received	E-mail	E-mail received date and time
Received Date	E-mail	E-mail received date
Date and Time Created	Non-e-mail	Date e-mail or application file was created
Date and Time Last Modified	Non-e-mail	Date e-mail or application file was last modified
Author	Non-e-mail	Author of the application file
From	E-mail	Sender of the e-mail
Recipient	E-mail	Recipients of the e-mail
Соруее	E-mail	CCs of the e-mail
BCC	E-mail	BCCs of the e-mail

Field Name	E-Mail or Non-E-Mail	Description
Directory/Folder Name	Both	Name of the folder (or folder structure) from where the file or e-mail was stored
File Extension/File Type	Both	Suffix to the name of the file; indicates the file format
File Size	Both	Document file size
Record Type	Both	Indicates whether document is an e-mail, attachment, or neither
Hash Value	Both	MDS or SHA-1 hash value used to deduplicate the data

Chapter 10

Predictive Coding and Computer-Assisted Document Review

Eric J. Mayer¹

§ 10.1 Introduction

With the explosive growth in digital information, practitioners and their clients need additional tools to help reduce the cost and time required to review and identify relevant documents in discovery. Predictive coding, now commonly referred to as technology-assisted review (TAR), is one such tool. It uses technologies from information retrieval science along with human input to more effectively and efficiently identify relevant (and nonrelevant) documents and reduce the time and cost involved in reviewing and producing electronically stored information (ESI). Predictive coding "has emerged as a far more accurate means of producing responsive ESI in discovery. Studies show it is far more accurate than human review or keyword searches, which have their own limitations."² Predictive coding can be used to identify and locate more than just relevant documents. With the proper training and input, more sophisticated predictive coding programs can identify and locate privileged documents, "hot documents," or other specific categories of documents of interest.

Predictive coding "is a type of machine-learning technology that enables a computer to automatically predict how documents should be classified based on limited human input."³ The process begins by having skilled attorneys review and code (for relevance, privilege, or some other category) a small number of documents called a "seed set" into a computer system. The coding decisions are then fed into the computer to create an algorithm that ranks and codes the remaining documents automatically.

Predictive coding may seem like exctic technology. It is not. Technology-assisted document review is something lawyers use every day. Most law firm e-mail systems

^{1.} The author would like to thank and acknowledge Rania Mohsen for her assistance in the preparation of this article.

^{2.} Progressive Cas. Ins. Co. v. Delaney, No. 2:11-CV-00678-LRH, 2014 WL 3563467, at *8 (D. Nev. July 18, 2014).

^{3.} Matthew Nelson, *Shining a Light into the Black Box of E-Discovery Predictive Coding*, Corporate Counsel (May 29, 2012), www.law.com/ccrpcounsel/almID/1202556081861/.

use filters to identify and then segregate junk or other unwanted e-mails. That useful and important technology is a species of predictive coding. These filters examine incoming digital information based on specific information provided by human programmers, and through the use of that information, algorithms in the software then rank and filter the digital information into relevant or nonrelevant categories.

§ 10.2 Need for Experienced Specialist

Predictive coding should only be done with the assistance of an experienced e-discovery specialist. All e-discovery vendors now offer predictive coding. Using an experienced e-discovery vendor is essential for two reasons. First, most predictive coding programs use proprietary technology, and the products can be used only by agreement or license, which is obtained through e-discovery vendors. Second, successful use of predictive coding requires the implementation of a system that can validate and verify the accuracy of the predictive coding search technology. An experienced e-discovery vendor can design and implement such a system.

Practitioners should also understand that technology and product offerings in this area change and improve constantly. For this reason, some e-discovery vendors license what they believe is the best current technologies and offer those to their customers. Other e-discovery vendors have opted to invest in and develop their own proprietary (and often patented) technology. For these reasons, before selecting an e-discovery vendor to employ predictive coding, practitioners should consult with more than one e-discovery vendor, investigate current technologies, and collect competitive bids. In so doing, request the names and contact information of previous customers and interview them regarding their experience with the vendor and program under consideration. (The authors of this chapter are not associated with any e-discovery company or program, and accordingly, no one vendor or platform is recommended in this chapter.)

§ 10.3 Skilled Attorney Review Essential

Predictive coding requires active involvement and input by skilled human reviewers. For predictive coding to work, an experienced attorney familiar with the case and issues presented in the litigation must train the software to recognize and locate relevant documents. This is done by having the attorney go through a subset of the documents assembled for review. This subset is the seed set. The attorney reviews documents in the seed set and identifies or codes them into specific categories, like relevant or responsive, or nonrelevant or nonresponsive. Those coding decisions are then used to teach the software to recognize (and code) the remaining documents similarly so that large quantities of ESI can be quickly, economically, and accurately reviewed.

§ 10.4 Not Appropriate for All Cases

Predictive coding is not recommended for all litigation. Currently, due to the cost associated with predictive coding technology, most e-discovery vendors do not recommend its use in cases where fewer than 150,000 documents need to be reviewed. Nor are cases with large quantities of graphic documents, spreadsheets, or nontextual materials good candidates for predictive coding, because existing software does not lend itself to identifying these types of nontextual, non-English ESI.

§ 10.5 Benefits

Advocates of predictive coding claim that it combines the best of two features: (1) an automated review process and (2) experienced human review. Unlike keyword searches followed by a manual review by scores of individual contact attorneys, predictive coding uses manual review by a small team of experienced attorneys with a small group of seed set documents. Once this process identifies relevant and important documents, technology is used to automatically replicate finding those documents. The computer automatically categorizes and prioritizes documents based not just on keyword frequency, but also on other qualities like document type, language, content, party, time frame, individual name, and concept meaning. These attributes allow the computer to group and prioritize similar documents in a more accurate and consistent manner than teams of human reviewers can. Studies have indicated that when performed correctly, predictive coding is more accurate than traditional manual review in locating and identifying relevant documents. This is attributed to the use of complex algorithms in a more predictable review process, which is less prone to human error or variation.⁴

In the proper case, and with appropriate training and implementation, predictive coding allows the practitioner to review large quantities of ESI more quickly and cheaply than the cost of linear (manual) review. One e-discovery vendor claims that its predictive coding technology, properly trained and administered, will accurately review and rank ESI for relevance at speeds of 150,000 documents per hour. At this pace, millions of documents can be accurately reviewed and ranked for relevance in just a mat-

^{4.} Charles Yablon & Nick Landsman-F.oos, Predictive Coding: Emerging Questions and Concerns, 64 S.C. L. Rev. 633, 678 (2013).

ter of days, during which, according to this e-discovery vendor, large quantities of nonrelevant materials are also identified and eliminated from further review. Since reviewing documents for relevance can be one of the single biggest costs in discovery,⁵ predictive coding is a tool that practitioners need to understand and consider.

Predictive coding offers other benefits. Predictive coding can be used to provide practitioners with early insight into key issues in their case. Identifying the controlling issues of a case at the outset of the litigation allows a skilled attorney (armed with predictive coding technology) to locate and review the most important documents early in a case. This then allows an attorney to provide clients focused early legal analysis and risk assessment-real benefits to litigants. Finally, predictive coding allows for new and additional materials to be reviewed efficiently and accurately. Most cases evolve with time, and issues and claims may change as the litigation matures. Predictive coding is designed to allow new ESI to be added and then reviewed and coded quickly and efficiently, all at a fraction of the cost of manual review.

§ 10.6 Building the Seed Set

Currently, there are two accepted methods of building the seed set: (1) random selection and (2) judgmental or subjective selection. Random selection is just that, a predetermined number of documents from the total universe of documents randomly selected for inclusion in the seed set. These documents are then coded or categorized into specific categories like "responsive," "nonresponsive," "privileged," "hot," or any similar variation. This process is typically done by a manual review of the seed set by an experienced attorney knowledgeable about the litigation.

The second accepted method involves more subjective decisions by those involved in the process. Under this method, attorneys with knowledge of the case specifically select documents for inclusion in the seed set because they represent categories of documents the attorneys feel are representative of issues in the case and are clear examples of relevant, nonrelevant, privileged, or hot documents. Proponents of this method believe that predictive coding works best with a "rich" seed set—a seed set intentionally full of relevant and case-specific documents—because training the predictive coding software is easier and more efficient. The type of seed set that works best will depend on the volume of material to be reviewed, the complexity of the

^{5.} See Nicholas M. Pace & Laura Zakaras, Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery, p. 97 (RAND Institute for Civil Justice 2012), www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1208.pdf.

issues involved, input from your predictive coding e-discovery specialist, and your familiarity with the process and the specific algorithm used.⁶

§ 10.7 Culling Is Required

Before creation of the seed set, culling is necessary. ESI will frequently contain duplicates of e-mails, documents, spreadsheets, and other digital information. There is no reason to spend time and money using predictive coding on duplicates. Before creation of the seed set, both vertical (within a single custodian's documents) and horizontal (across all custodians) deduplication needs to occur. Your e-discovery vendor can assist with this essential step. Given the availability of commercial deduplication programs, your client's internal IT department may also be able to perform this essential step.

§ 10.8 Training the Computer

Because predictive coding requires skilled human intervention and input, it is an interactive and iterative process. Skilled document reviewers familiar with the case review the seed set and categorize the documents. Algorithms contained in the software then create a model to be used to analyze other documents. The algorithm typically assigns a numerical score to each document that reflects the probability that the document fits within the model. Attorneys then take this random set of ranked documents and manually examine them to see how well the computer algorithm captured the issues "taught" by the reviewers. In other words, did the algorithm correctly determine the relevant and nonrelevant documents? This interactive examination must be repeatedly performed to ensure that the algorithm used by the computer is effective in finding and categorizing the documents. The algorithm must then be tested on a control set. This is typically done by selecting a random set of documents separate and apart from the seed set and having the predictive coding software attempt to identify the relevant documents in this control set. The output of the control set analysis are examined by a skilled attorney document reviewer to see if the software is correctly identifying relevant documents and correctly identifying or predicting the other document categories (nonrelevant and privileged). This is a continuing process and must be performed until the algorithm is deemed accurate enough so that when run against a control set, it will predict a certain percentage of the categories correctly. This measure of accuracy is sometimes known as precision, that is, the percentage of docu-

^{6.} See Charles Yablon & Nick Landsman-Roos, *Predictive Coding: Emerging Questions and Concerns*, 64 S.C. L. Rev. 633 (2013) at 639 for a more in-depth discussion of different types of seed sets.

ments identified as relevant by a review effort that are in fact relevant. To summarize, the seed set is used to train the computer while the control set is used to measure accuracy of the predictive coding algorithm.⁷

§ 10.9 Quality Control

For predictive coding to be effective and usable there must be a way to test whether the system predictions are accurate. This is typically done by examining the control set of documents and checking the accuracy of calls made within that set of the materials. All categories should be reviewed for accuracy. Documents deemed nonresponsive should be sampled to ensure that the relevance categorizations were accurately done. This is particularly important because predictive coding documents categorized as nonresponsive or irrelevant rarely get reviewed again. Responsive or relevant documents are typically reviewed before they are produced, thus providing a de facto quality check on this category.⁸ Privileged documents are also typically manually reviewed and logged, thus providing assurance that the categorizations were accurately done.

§ 10.10 How Predictive Coding Software Works

Predictive coding technology is proprietary. For that reason, information on exactly how the software works is not often public or available. In all cases, this proprietary software requires attorney input to predict how certain documents in the larger universe of documents will be coded or categorized. Some algorithms look at only the text used and then attempt to predict similar documents based on textual patterns. Other software algorithms analyze the metadata contained in a document along with the text. Examples of predictive coding algorithms include—

- *Nearest Neighbor:* a supervised learning algorithm in which a new document is classified by finding the most similar document in the training set.
- Support Vector Machine: a state-of-the-art supervised learning algorithm that separates relevant from nonrelevant documents by using geometric methods. Each document is considered to be a point in space whose coordinates are determined by the features contained in the document. The machine then looks at the training set and determines the plane that best

^{7.} Yablon & Landsman-Roos, Predictive Coding at 640.

^{8.} Daniel B. Garrie & Yoav M. Griver, *Unchaining E-Discovery in the Patent Courts*, 8 Wash. J.L. Tech. & Arts 487 (2013).

separates the relevant from the nonrelevant document and uses that geometric plane to identify documents in the general population depending on which side of the geometric plane the documents fall into.

• *Bag of Words:* an algorithm that categorizes each document as a set of specific words. Documents are then chosen as relevant or nonrelevant depending on the Bag of Words they contain.

§ 10.11 Example of the Process

Predictive coding requires a detailed and specific protocol. Practitioners contemplating its use should review the case management orders from *Rio Tinto PLC v. Vale S.A.*⁹ and *In re Actos (Pioglitazone) Prod. Liab. Litig.*¹⁰ In both cases, the parties worked together to create an agreed upon predictive coding protocol. The protocols explain exactly how the parties (1) created their seed set, (2) trained the predictive coding software, (3) handled privileged information from the seed set, and (4) verified the accuracy of the predictive coding software used.

§ 10.12 Producing Documents

Once the predictive coding software has been sufficiently trained so that the attorneys are comfortable with its results and the materials are reviewed, the attorneys in charge of the document review process have several options. They can manually review all documents selected as relevant and then produce the non-privileged documents to their opponent; another option is simply to produce all documents above a threshold relevancy percentage with a snap-back order allowing for return of any privilege documents without waiver of privilege (see chapter 12 of this book). Documents below a certain relevancy score are typically deemed irrelevant and thus not produced. Documents deemed nonresponsive should be sampled to ensure that the relevance categorizations were accurately done.

§ 10.13 Seed Set Disclosure

The most significant discovery issue associated with predictive coding is the extent to which the seed set must be shared with your opponent. Most of the published judicial

^{9. 306} F.R.D. 125 (S.D.N.Y. 2015) (Stipulation and Order Re: Use of Predictive Coding in Discovery).

^{10.} No. 6:11-md-2299, 2012 WL 6061973 (W.D. La. July 27, 2012) (Case Management Order: Protocol Relating to the Production of Electronically Stored Information ("ESI")).

opinions on predictive coding (see section 10.15 below) advocate transparency and thus encourage disclosure of the seed set. The type of seed set used (random versus judgmental) is also impacted. A random seed set does not disclose attorney-work product, while a judgmental seed set would, because it involves the selection of certain documents deemed to be representative of issues in the case. One possible solution is to have the parties agree to build the seed set collaboratively. That is precisely the methodology agreed to by the parties in the *In re Actos* case management order and in the *Rio Tinto* stipulation and order.¹¹ For example, in *In re Actos* the parties agreed to each appoint three experts specifically to create a seed set and to then train the predictive coding software used in the case.

While courts continue to encourage increased transparency, case law is split on how to proceed when the parties cannot agree on the degree of transparency. Some courts have not required disclosure, but have still encouraged it.¹² Some courts have required disclosure,¹³ and one court cited a lack of cooperation and transparency as a reason to disallow the use of TAR where such use would deviate from an already agreed upon ESI protocol.¹⁴

Overall, courts encourage transparency but have generally avoided mandating the technical aspects of TAR, such as whether parties have to provide seed sets or their audit practices, and by establishing "confidence levels" (see next section).¹⁵ Instead, parties are encouraged to create an agreed upon protocol.¹⁶ One court noted that if par-

13. See record transcript for Fed. Hous. Fin. Agency v. JPMorgan Chase & Co., No. 1:11-cv-06188-DLC, 2014 WL 584300 (S.D.N.Y. July 24, 2012).

14. See Progressive Cas. Ins. Co. v. Delaney, No. 2:11-CV-00678-LRH, 2014 WL 3563467 (D. Nev. July 18, 2014) (Progressive's unwillingness to engage in transparency and cooperation resulted in the denial of its predictive coding proposal).

15. Ronald L. Johnston, *Court Guideposts for the Path to Technology Assisted Review Adoption*, The Computer & Internet Lawyer (Vol. 35 No. 2, Feb. 2018) www.bakerlaw.com/webfiles/Litigation/ 2018/Articles/2018-02-01-The-Computer-And-Internet-Lawyer.pdf, at 6.

^{11.} See In re Actos (Pioglitazone) Prod. Liab. Litig., No. 6:11-md-2299, 2012 WL 6061973 (W.D. La. July 27, 2012); Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125 (S.D.N.Y. 2015).

^{12.} See In re Biomet M2a Magnum Hip Implant Prod. Liab. Litig., No. 3:12-MD-2391, 2013 WL 6405156 (N.D. Ind. Aug. 21, 2013) (court concluded that it did not have the "authority to compel" discovery of non-responsive seed set materials, but noted that Biomet's level of cooperation was below what the Sedona Conference endorses); see also Aurora Coop. Elevator Co. v. Aventine Renewable Energy-Aurora W., LLC, No. 4:12CV230, 2015 WL 10550240 (D. Neb. Jan. 6, 2015) (court declined to require defendants to produce irrelevant documents stating defendants' argument against production was supported by the rules of procedure, but encouraged the defendants to "reconsider their position and work cooperatively"); Entrata, Inc. v. Yardi Sys., Inc., No. 2:15-CV-00102, 2018 WL 5470454 (D. Utah Oct. 29, 2018) (court declined to require plaintiff to produce "the complete methodology and results of" its TAR process stating that the defendants provided no specific examples of deficiencies in Plaintiff's document production or "more detailed reasons" why TAR information was needed).

ties can't cooperate and work together, requesting parties have other ways to make sure TAR is implemented appropriately, including checking statistical recall percentages, noting gaps in production, and a quality control review of sample documents categorized as nonresponsive.¹⁷

§ 10.14 Measuring Accuracy

The accuracy of any predictive coding system is paramount. Without reliable data to indicate it is working correctly, the user of predictive coding cannot demonstrate to the court or opponent that the system is accurately locating the responsive material requested. Sometimes known as "confidence levels," these percentages are typically used to evaluate the effectiveness of any predictive coding methodology. The parties will likely have different views on what constitutes an appropriate confidence level. The party producing documents may want a lower percentage (for example, 90 percent) while a party requesting documents will typically want something higher (for example, 99 percent). A related issue is relevancy threshold-at what point are documents deemed irrelevant? For example, the parties could agree that all documents that are scored 7 or above by the predictive coding software should be produced and that documents scored 4 or below should not be produced. What about the documents scored between 4 and 7? The parties may have differing views on how those documents should be treated. Plaintiffs may want production of these documents while defendants may want them excluded as irrelevant. The parties could ask for court intervention, but there are other options. For example, documents scored 5 or 6 could be reviewed either manually or through some sampling technique to ensure that relevant and responsive materials are not being excluded from review. Again, these are issues that are best worked out by the parties. However, in the absence of agreement, courts will and have begun ruling on these issues.

§ 10.15 Developing Case Law

Until 2012 there were no reported decisions that addressed the use of predictive coding in state or federal courts. In 2012, five reported cases addressed various issues surrounding the use of predictive coding. They are discussed briefly in this section along with the significance each presents. At the time this book was updated in 2020, several more cases have dealt with these issues as well.¹⁸

^{16.} See, e.g., Winfield v. City of New York, 15-CV-05236 LTSKHP, 2017 WL 5664852 (S.D.N.Y. Nov. 27, 2017).

^{17.} Rio Tinto PLC, 306 F.R.D. at 128-129.

§ 10.15:1 Da Silva Moore

In *Da Silva Moore v. Publicis Groupe*, 287 F.R.D. 182 (S.D.N.Y 2012), the use of predictive coding in a federal class action discrimination case in New York was approved. The plaintiffs brought claims against their employer under title VII of the Civil Rights Act, the Equal Pay Act, and later the Fair Labor Standards Act. The defendant wanted to use predictive coding to control the cost of producing relevant ESI. The defendant believed he could produce documents in this class action for no more than \$200,000, but to do so he would need to use predictive coding. The plaintiffs objected. Over the plaintiffs' objections, Magistrate Judge Andrew Peck authorized the use of predictive coding at the initial stages of the litigation with a caveat that if the predictive coding results proved unsatisfactory, the plaintiffs were free to return to the court and seek additional discovery. *Da Silva Moore* is the first federal case authorizing the use of predictive coding over a plaintiff's objection.

Although much is often said about this case, it is significant to note that many of the specific issues that divide parties on the use of predictive coding (confidence level and precision required) were not specifically decided by the court. In other words, the court did not decide, for example, that an acceptable confidence level would be 92 percent or that all documents ranked below 4 are nonresponsive. Rather, the decision was a tentative one, issued at the early stages of the case with the understanding that predictive coding was an untested technology that would certainly require fine-tuning by the parties and the court as the case progressed.

In ordering the use of predictive coding over the plaintiffs' objections, the court validated this document collection and production technique and cited studies that indicated predictive coding was more reliable and cost-effective than a keyword and manual document review. Judge Peck refused to impose specific requirements on quality control, holding instead that the defendant could proceed with its predictive coding protocol, but that the plaintiffs reserved their right to challenge the thoroughness of the document collection and production process at a later date. The plaintiffs' objections to the use of the technology before the establishment of specific relevancy

^{18.} See Dynamo Holdings L.P. v. Comm'r, 143 T.C. 183 (2014); Progressive Cas. Ins. Co. v. Delaney, No. 2:11-CV-00678-LRH, 2014 WL 3563467 (D. Nev. July 18, 2014); In re Biomet M2a Magnum Hip Implant Prod. Liab. Litig., No. 3:12-MD-2391, 2013 WL 6405156 (N.D. Ind. Aug. 21, 2013); Aurora Coop. Elevator Co. v. Aventine Renewable Energy-Aurora W., LLC, No. 4:12CV230, 2015 WL 10550240 (D. Neb. Jan. 6, 2015); Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125 (S.D.N.Y. 2015); Hyles v. New York City, No. 10 Civ. 3119, 2016 WL 4077114 (S.D.N.Y. Aug. 1, 2016); In re Viagra (Sildenafil Citrate) Prod. Liab. Litig., No. 16-MD-02691-RS(SK), 2016 WL 7336411 (N.D. Cal. Oct. 14, 2016); Winfield v. City of New York, 15-CV-05236 LTSKHP, 2017 WL 5664852 (S.D.N.Y. Nov. 27, 2017); Entrata, Inc. v. Yardi Sys., Inc., No. 2:15-CV-00102, 2018 WL 5470454 (D. Utah Oct. 29, 2018).

benchmarks and confidence levels were rejected. Judge Peck brushed aside these objections by finding that the plaintiffs' interests were adequately protected because they could return to challenge the document collection process and, significantly, that the predictive coding protocol proposed by the defendant allowed for total transparency. The plaintiffs would be entitled to see how the defendant coded each e-mail or document used in this seed set. Since *Da Silva Moore*, several cases have allowed or approved the use of TAR in the discovery process.¹⁹

§ 10.15:2 Kleen Products

In *Kleen Products LLC v. Packaging Corp. of America*, No. 10 C 5711, 2012 WL 4498465 (N.D. Ill. Sept. 28, 2012), an antitrust suit involving alleged price fixing in the container board industry, the plaintiffs asked the court to order the defendants to use predictive coding even though the defendants had already begun producing documents. Relying on Sedona Principle 6, the court refused the plaintiffs' request to require the defendants to use predictive coding, holding that the defendants' choice of methodology (keyword searching) was not unreasonable and that unless the plaintiffs could show that the process used by the defendants was inadequate, the defendants were entitled to proceed with the method of their choosing.²⁰ *Kleen Products* makes clear that Sedona Principle 6 allows the producing party to select and use a method of document collection and production of its choosing, and indicates that without a showing that the chosen methodology is inherently unreasonable or unreliable, an objecting party cannot require the use of predictive coding even if it believes that methodology is more accurate and cost-effective.

In a 2016 case out of the Southern District of New York, Judge Andrew J. Peck made it clear that the court "cannot, and will not" force a producing party to use predictive coding. *Hyles v. New York City*, No. 10 CIV 3119 (AT)(AJP), 2016 WL 4077114 (S.D.N.Y. Aug. 1, 2016), involved a racial discrimination suit. A TAR issue arose

^{19.} See Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125 (S.D.N.Y. 2015); Dynamo Holdings L.P. v. Comm'r, 143 T.C. 183 (2014); In re Viagra (Sildenafil Citrate) Prod. Liab. Litig., No. 16-MD-02691-RS(SK), 2016 WL 7336411 (N.D. Cal. Oct. 14, 2016); In re Biomet M2a Magnum Hip Implant Prod. Liab. Litig., No. 3:12-MD-2391, 2013 WL 6405156 (N.D. Ind. Aug. 21, 2013); Aurora Coop. Elevator Co. v. Aventine Renewable Energy-Aurora W., LLC, No. 4:12CV230, 2015 WL 10550240 (D. Neb. Jan. 6, 2015); Winfield v. City of New York, 15-CV-05236 LTSKHP, 2017 WL 5664852 (S.D.N.Y. Nov. 27, 2017); Entrata, Inc. v. Yardi Sys., Inc., No. 2:15-CV-00102, 2018 WL 5470454 (D. Utah Oct. 29, 2018).

^{20.} See Kleen Products, 2012 WL 4498465, at *5 ("[U]nder Sedona Principle 6, '[r]esponding parties are best situated to evaluate the procedures, methodologies, and techniques appropriate for preserving and producing their own electronically stored information."") (citing The Sedona Conference, *The Sedona Conference Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, 15 Sedona Conf. J. 222, 226 (2014)).

when discovery got underway. The issue was whether the defendant could be forced, at Plaintiff's request, to use TAR when it preferred to use keyword searching. While the court stated that "in general, TAR is cheaper, more efficient and superior to keyword searching," it relied on Sedona Principle 6 when refusing to compel the producing party's use of TAR.²¹ "There may come a time when TAR is so widely used that it might be unreasonable for a party to decline to use TAR. We are not there yet."²²

In re Viagra (Sildenafil Citrate) Prod. Liab. Litig., No. 16-MD-02691-RS(SK), 2016 WL 7336411 (N.D. Cal. Oct. 14, 2016), another 2016 decision, agreed with *Hyles*' reasoning, and the court refused to compel the producing party to use a particular form of ESI retrieval. In that case, the plaintiffs urged the court to compel defendant Pfizer to use TAR, arguing that it was a more sophisticated tool that would save money for both sides. Pfizer instead wanted to use search terms. The court concluded that "even if predictive coding were a more efficient and better method," the court had no basis to compel Pfizer to use predictive coding, especially without any evidence that Pfizer's chosen method would result in insufficient discovery responses.²³

§ 10.15:3 Global Aerospace

In Global Aerospace Inc. v. Landow Aviation, No. CL 61040, 2012 WL 1431215 (Va. Cir. Ct. Apr. 23, 2012), litigation resulted following the collapse of three hangars at the Dulles airport during a snowstorm in 2010. Several suits were filed and consolidated for discovery purposes. The defendant wanted to use predictive coding to produce documents to control costs. The plaintiff objected, requiring the defendant to move for a protective order on the use of predictive coding. The defendant argued that a manual review of documents requested would cost more than \$2 million and would at best locate only 60 percent of relevant documents. The defendant supported this assertion by citing studies showing that linear (manual) document reviews were not very accurate and that in this case predictive coding could get 75 percent of the relevant documents at a fraction of the costs required for manual review. The defendant also proposed a predictive coding protocol with significant transparency, including an agreement to produce the seed set and virtually all materials used to train the predictive coding software. The only materials that would not be provided to the plaintiff were privileged or commercially sensitive documents in the seed set. Those materials would be logged, however, and a copy of that log would be provided to the plaintiff.

- 22. Hyles, 2016 WL 4077114 at *3.
- 23. In re Viagra, 2016 WL 7336411 at *2.

^{21.} Hyles, 2016 WL 4077114 at *2.

The plaintiff objected, arguing that there were not adequate grounds to justify the defendant's departure from traditional manual review. The plaintiff argued that any computer-assisted technology should be used to supplement traditional manual review and not replace it.

The plaintiff lost. The state court judge approved the defendant's use of predictive coding "for the purpose of processing and production of electronically stored information."²⁴ But, as in the other cases discussed above, the court left open the possibility that the plaintiff could return to the court to seek an adjustment if the predictive coding technology and protocol proved ineffective. The court's rationale can be explained by reliance on Sedona Principle 6, which affords a strong presumption that the methodology chosen by the producing party will not be disturbed absent a significant showing of unreliability. *Global Aerospace* is the first published state court opinion authorizing the use of predictive coding.

§ 10.15:4 In re Actos

In re Actos consists of multidistrict litigation over the Actos prescription drug.²⁵ Eleven separate cases were consolidated before Magistrate Judge Doherty of the Western District of Louisiana. In July of 2012, Judge Doherty entered a case management order including a detailed protocol for the production of electronically stored information. Here, the parties agreed on the use of predictive coding and also agreed on a very detailed order specifically spelling out how documents were to be collected, how the seed set and training were to occur, and how the parties were to decide on scores for establishing relevancy. Because of its detail, a copy of that case management order should be reviewed by practitioners contemplating use of predictive coding.

§ 10.15:5 EORHB, Inc. v. HOA Holdings LLC

EORHB, Inc. v. HOA Holdings LLC, No.7409-VCL, 2012 WL 4896670 (Del. Ch. Oct. 15, 2012), also known as the "Hooters case," involves an indemnity dispute following the sale of the Hooters restaurant chain. It is significant because it is the first reported decision where predictive coding document review was ordered by the trial court sua sponte.²⁶ In this case, Delaware Vice Chancellor Travis Laster ordered the

^{24.} Global Aerospace, 2012 WL 1431215.

^{25.} See In re Actos, No. 6:11-md-2299, 2C12 WL 6061973 (W.D. La. July 27, 2012).

^{26.} EORHB, 2012 WL 4896670, at *1.

parties to use predictive coding after determining that large quantities of ESI were likely to be produced by both sides in the litigation. Without either party requesting the use of this technology, Chancellor Laster ordered the parties to "(i) retain a single discovery vendor to be used by both sides, and (ii) conduct document review with the assistance of predictive coding."²⁷ Approximately one year later, Chancellor Laster took a different approach. In May of 2013, based on an agreed proposal from the parties, Chancellor Laster entered a new order allowing the parties to "conduct document review using traditional methods," withdrawing his earlier order requiring predictive coding.²⁸

These cases demonstrate that state and federal courts are moving to embrace predictive coding but are doing so in a way that allows the objecting party to challenge the production if it can show that predictive coding proves unreliable. The decisions demonstrate the importance of Sedona Principle 6, which allows the producing party to decide on the methodology best suited to review, select, and produce documents. Finally, the cases make clear that predictive coding will certainly require transparency. Seed sets and all materials used in the training of the predictive coding software, including nonresponsive documents, may have to be shared with your opponent. Sensitive or privileged materials may need to be provided or at least logged.

§ 10.16 Conclusion

Predictive coding, or TAR, is a recognized and acceptable tool to review and produce documents in certain cases. Today, TAR is widely accepted by courts, though it is still not mandatory.²⁹ When a producing party wants to use TAR, courts will generally allow it even over an objection by the other party.³⁰ However, if one side wants to depart from an already agreed upon protocol or methodology for the production of ESI, then an agreement to deviate from the protocol may be necessary.³¹ Finally, most courts will not require a party to use TAR, notwithstanding a demand by the requesting party.³²

30. Rio Tinto PLC v. Vale S.A., 306 F.R.D. 125, 127 (S.D.N.Y. 2015).

31. Progressive Cas. Ins. Co. v. Delaney, No. 2:11-CV-00678-LRH, 2014 WL 3563467, at *9 (D. Nev. July 18, 2014).

^{27.} EORHB, 2012 WL 4896670.

^{28.} EORHB, Inc. v. HOA Holdings LLC, C.A. No. 7409-VCL, 2013 WL 1960621, at *1 (Del. Ch. May 6, 2013).

^{29.} *Rio Tinto PLC v. Vale S.A.*, 306 F.R.D. 125, 127 (S.D.N.Y. 2015) (court noting that in the years since the Da Silva Moore ruling, "[c]ase law has developed to the point that it is now black letter law that where the producing party wants to utilize TAR for document review, courts will permit it.").

TAR's use and acceptance will certainly continue to increase as its benefits and cost savings become more widespread and clients and practitioners continue to seek new tools to control the time and costs associated with ESI discovery.

^{32.} Hyles v. New York City, No. 10 Civ. 3119, 2016 WL 4077114, at *1 (S.D.N.Y. 2016).



Chapter 11

Processing in E-Discovery, a Primer

Craig Ball

§ 11.1 Introduction

Talk to lawyers about e-discovery processing and you'll likely get a blank stare. Why would lawyers want anything to do with something so disagreeably technical? Indeed, processing is technical and strikes attorneys as something they need not know. This is lamentable because processing is a stage of e-discovery where things can go terribly awry in terms of cost and outcome. Lawyers who understand the fundamentals of electronically stored information (ESI) processing are better situated to avoid costly mistakes and resolve them when they happen. This chapter looks closely at ESI processing and seeks to unravel its mysteries.

Processing is the "black box" between preservation/collection and review/analysis. Though the iconic Electronic Discovery Reference Model (EDRM) positions processing, review, and analysis as parallel paths to production, processing is an essential prerequisite—"the only road"—to review, analysis, and production. Remember, EDRM is a conceptual view, not a workflow. Any way you approach e-discovery at scale, you must process ESI before you can review or analyze it. If we recast the EDRM to reflect processing's centrality, the famed schematic would look like the figure below.



There are hundreds—perhaps thousands—of articles delving into the stages of e-discovery that flank processing in the EDRM. These are the stages where lawyers have had a job to do. But lawyers tend to cede processing decisions to technicians. When it comes to processing, lawyer competency and ken is practically non-existent, little

more than "stuff goes in, stuff comes out."

§ 11.2 Why Process ESI in E-Discovery? Isn't It "Review-Ready?"

We process information in e-discovery to catalog and index contents for search and review. Unlike Google, e-discovery is the search for all responsive information in a collection, not just one information item deemed responsive. Though all ESI is inherently electronically searchable, computers don't structure or search all ESI in the same way; therefore we must process ESI to *normalize* it to achieve uniformity for indexing and search.

Thus, processing in e-discovery could be called "normalized access" in the sense of extracting content, decoding it, and managing and presenting content in consistent ways for access and review. Processing encompasses the steps required to extract text and metadata from information and build a searchable index. The closest analogy is the creation of a Google-like capability with respect to a discrete collection of documents, data and metadata.

ESI processing tools perform five common functions.¹ They must—

- 1. decompress, unpack and fully explore, i.e., recurse ingested items;
- 2. identify and apply templates (filters) to encoded data to parse (interpret) contents and extract text, embedded objects, and metadata;
- 3. track and hash items processed, enumerating and unitizing all items and tracking failures;
- 4. normalize and tokenize text and data and create an index and database of extracted information; and
- 5. cull data by file type, date, lexical content, hash value and other criteria.

These steps are a more detailed description of processing than most texts on the subject, but this chapter means to go deeper, diving into *how* it works and exposing situations where it may fail to meet expectations.²

^{1.} While a processing tool may do considerably more than the listed functions, a tool that does less is unlikely to meet litigants' needs in e-discovery.

§ 11.3 Files

If we polled lawyers and asked what to call the electronic items preserved, collected, and processed in discovery, most would answer "documents." Others might opt for "data" or reflect on the initialization "ESI" and say "information." None are wrong answers, but the ideal response would be the rarest: "files." Electronic documents are files; electronically stored information resides in files. Everything we deal with digitally in electronic discovery comes from or goes to physical or logical data storage units called "data files" or just "files." Moreover, all programs that are run against data files are themselves files comprising instructions for tasks. These are "executable files," or simply "executables."

So, what is it we process in the processing stage of e-discovery? The answer is that "we process files." Let's look at these all-important files and explore what's in them and how they work.

§ 11.3:1 A Bit About and a Byte Out of Files

A colleague of this chapter's author once defended her ignorance of the technical fundamentals of electronically stored information by analogizing that she didn't "need to know how planes stay aloft to fly on one." She had a point, but only for passengers. If you aspire to be a pilot or a rocket scientist—if you want to be at the controls or design the plane—you must understand the fundamentals of flight. If you aspire to understand the processing of ESI in e-discovery and manage e-discovery, you must understand the fundamentals of electronically stored information, including such topics as:

- What's store electronically?
- How is it stored?
- What forms does it take?

Chapter 4 of this book is a "crash course" in digital data, particularly the basics of encoding and recording textual information.

^{2.} The abandoned efforts of the EDRM to educate via their Processing Standards Guide are cornmendable, however it is still in its public comment phase more than five years after publication. www.edrm.net/resources/frameworks-and-standards/edrm-model/edrm-stages-standards/edrm -processing-standards-guide-version-1/.

The many ways in which data is encoded—and the diverse ways in which collection, processing, and search tools identify the multifarious encoding schemes—lie at the heart of significant challenges and costly errors in e-discovery. It's easy to dismiss these fundamentals of information technology as too removed from litigation to be worth the effort to explore, but understanding encoding and the role it plays in processing, indexing, and searching will help you realize the capabilities and limits of the tools you, your clients, vendors, and opponents use.

Let's look at these issues and file formats through the lens of a programmer making decisions about how a file should function.

§ 11.3:2 Hypothetical: TaggedyAnn

Ann, a programmer, must create a tool to generate nametags for attendees at an upcoming continuing legal education program. Ann wants her tool to support different label stock and multiple printers, fonts, font sizes, and salutations. The tool will accept lists of pre-registrants as well as create name tags for those who register onsite. Ann will call her tool TaggedyAnn. TaggedyAnn has never existed, so no computer operating system "knows" what to do with TaggedyAnn data. Ann must design the necessary operations and associations.

Remembering our mantra "ESI is just numbers," Ann must lay out those numbers in the data files so that the correct program—her TaggedyAnn program—will be executed against TaggedyAnn data files, and she must structure the data files so that the proper series of numbers will be pulled from the proper locations and interpreted in the intended way. Ann must develop the "file format."

A file format establishes the way to encode and order data for storage in the file. Ideally, Ann will document her file format as a published specification, a blueprint for the file's construction. That way anyone trying to develop applications to work with Ann's files will know what goes where and how to interpret the data. But Ann may never get around to writing a formal file specification or, if she believes her file format to be a trade secret, Ann may decide not to reveal its structure publically. In that event, others seeking to read TaggedyAnn files must reverse engineer the files to deduce their structure and fashion a document filter that can accurately parse and view the data.

In terms of complexity, file format specifications run the gamut. Ann's format will likely be simple—perhaps just a page or two—as TaggedyAnn supports few features and functions. By contrast, the published file specifications for the binary forms of

File Type Identification: In the context of the operating system, Ann must link her program and its data files through various means of file type identification. File type identification using binary file signatures and file extensions is an essential early step in e-discovery processing. Determining file types is a necessary precursor to applying the appropriate document filter to extract contents and metadata for populating a database and indexing files for use in an e-discovery review platform.

File Extensions: Because Ann is coding her tool from scratch and her data files need only be intelligible to her program, she can structure the files any way she wishes, but she must nevertheless supply a way for computer operating systems to pair her data files with only her executable program, or there's no telling what program might run. Word might open the data in a PDF file, but the result could be unintelligible.

File name extensions, or just "file extensions," are a means to identify the contents and purpose of a data file. Though executable files must carry the file extension EXE, any ancillary files Ann creates can employ almost any three-letter or number file extension Ann desires, so long as her choice doesn't conflict with one of the thousands of file extensions already in use. That means that Ann can't use TGA because it's already associated with Targa graphics files, and she can't use TAG because that signals a DataFlex data file. So Ann settles on TGN as the file extension for Taggedy-Ann files. That way, when a user loads a data file with the TGN extension, Windows can direct its contents to the TaggedyAnn application and not to another program that is unable to correctly parse the data.

Binary File Signatures: But Ann needs to do more. Not all operating systems employ file extensions, and because extensions can be absent or altered, file extensions aren't the most reliable way to denote the purpose or content of a file. Additionally, file names and extensions are system metadata, so they are not stored inside the file. Instead, computers store file extensions within the file table of the storage medium's file system. Accordingly, Ann must fashion a unique "binary header signature" that precedes the contents of each TaggedyAnn data file so that the contents are identifiable as TaggedyAnn data and directed solely to the TaggedyAnn program for execution.

Ann peruses the lists of file signatures available online and initially thinks she will use Hex 54 41 47 21 as her binary header signature because no one else appears to be using that signature and it corresponds to "TAG!" in ASCII. But after reflecting on the volume of highly compressible text that will comprise the program's data files, Ann instead decides to store the contents in a ZIP-compressed format, necessitating the binary header signature for TaggedyAnn's data files be 50 4B 03 04, PK... in ASCII. All files compressed with ZIP use the PK.. header signature because Phil Katz, the programmer who wrote the ZIP compression tool, chose to flag his file format with his initials.

How can Ann ensure that only TaggedyAnn opens these files and they are not misdirected to an unzipping (decompression) program? Simple. Ann will use the TGN extension to prompt Windows to load the file in TaggedyAnn, and TaggedyAnn will then read the PK.. signature and unzip the contents to access the compressed contents.

But what about when an e-discovery service provider processes the TaggedyAnn files with the mismatched file extensions and binary signatures? Wouldn't this throw things off? It could. We'll return to that issue when we cover compound files and recursion later in this chapter. First, let's touch on file structures.

File Structure: Now Ann must decide how she will structure the data within her files. Once more, Ann's files need only be intelligible to her application, so she is unconstrained in her architecture. This point becomes important since the differences in file structure are what make processing and indexing essential to electronic search. There are thousands of different file types, each structured in idiosyncratic ways. Processing normalizes their contents into a common searchable format.

§ 11.4 Data Compression

Many common file formats and containers are compressed, necessitating that e-discovery processing tools be able to identify compressed files and apply the correct decompression algorithm to extract contents.

Compression is miraculous. It makes modern digital life possible. Without compression, we wouldn't have smart phones, digitized music, streaming video, or digital photography. Without compression, the web would be a different, duller place.

Compression uses algorithms to reduce the space required to store and the bandwidth required to transmit electronic information. If the algorithm preserves all compressed

data, it's termed "lossless compression." If the algorithm jettisons data deemed expendable, it's termed "lossy compression."

JPEG image compression is lossy compression, executing a tradeoff between image quality and file size. Not all of the original photo's graphical information survives JPEG compression. Sharpness and color depth are sacrificed, and compression introduces distortion in the form of rough margins called "jaggies." We likewise see a loss of fidelity when audio or video data is compressed for storage or transmission (e.g., as MPEG or MP3 files). The offsetting benefit is that the smaller file sizes facilitate streaming video and the storing of thousands of songs in your pocket.

ZIP employs a lossless compression algorithm called DEFLATE, which came into use in 1993. DEFLATE underpins both ZIP archives and the PNG image format, and thanks to its efficiency and it being free to use without license fees, DEFLATE remains the most widely used compression algorithm in the world.

Tools for processing files in e-discovery must identify compressed files and apply the correct algorithm in order to unpack the contents. The decompression algorithm locates the tree and symbols library and retrieves and parses the directory structure and stored metadata for the contents.

§ 11.5 Identification on Ingestion

Remember programmer Ann and her struggle to select a TaggedyAnn file extension and signature? Now those decisions play a vital role in how an e-discovery processing tool extracts text and metadata. If we hope to pull intelligible data from a file or container, the first step is to reliably ascertain the file's structure and encoding. For compressed files, apply the proper decompression algorithm. If it's an e-mail container format, apply the proper encoding schema to segregate messages and decode all manner of attachments. Treat image files as images, sound files as sounds, and so on. Misidentification of file types guarantees failure.

The e-discovery industry relies on various open source and commercial file identifier tools. These tend to look first at the file's binary header for file identification and then at the file's extension and name. If the file type cannot be determined from the signature and metadata, the identification tool might either flag the file as unknown (an "exception") or pursue other identification methods like byte frequency analysis (BFA) or the use of specialty file type detection tools designed to suss out characteristics unique to certain file types, especially container files. Identification tools will typically report both the apparent file type (obtained from metadata, like the file's name

and extension) and the actual file type. Inconsistencies between these may prompt special handling or signal spoofing with malicious intent.

§ 11.6 Media (MIME) Type Detection

File extensions are largely unique to Microsoft operating systems. Systems like Linux and Mac OS X don't rely on file extensions to identify file types. Instead, they employ a file identification mechanism called Media (MIME) Type Detection. MIME, which stands for Multipurpose Internet Mail Extensions, is a seminal Internet standard that enables the grafting of text enhancements, foreign language character sets (Unicode), and multimedia content (e.g., photos, video, sounds, and machine code) onto plain text e-mails. Virtually all e-mail travels in MIME format.

The ability to transmit multiple file types via e-mail created a need to identify the content type transmitted. The Internet Assigned Numbers Authority (IANA) oversees global Internet addressing and defines the hierarchy of media type designation. These hierarchical designations for e-mail attachments conforming to MIME encoding came to be known as "MIME types." Though the use of MIME types started with e-mail, elements like operating systems, tools, and web browsers now employ MIME types to identify media, which prompted the IANA to change the official name from MIME Types to Media Types.

Media types serve two important roles in e-discovery processing. First, they facilitate the identification of content based on a media type declaration found in things like email attachments and Internet publications. Second, media types serve as standard classifiers for files after the identification of content. Classification of files within a media type taxonomy simplifies culling and filtering data in ways useful to e-discovery. While it's enough to specify "document," "spreadsheet," or "picture" in a request for production, e-discovery tools require a more granular breakdown of content. Tools must be able to distinguish a Word binary DOC format from a Word XML DOCX format, a Microsoft PowerPoint file from a Mac Keynote file, and a GIF from a TIFF.

§ 11.6:1 Media Type Tree Structure

Media types follow a path-like tree structure under one of the following standard types: application, audio, image, text, and video (collectively called discrete media types) and message and multipart (called composite media types). These top-level media types are further defined by subtype and, optionally, by a suffix and parameter(s) written in lowercase.

Examples of file type declarations for common file formats

Note: file types prefixed by x- are not IANA.

Those prefixed by vnd. are vendor-specific formats.

Application	
Word DOC	application/msword
Word DOCX	application/vnd.openxmlformats-
	officedocument.wordprocessingml.document
Adobe PDF	application/pdf (.pdf)
PowerPoint PPT	application/vnd.ms-powerpoint
PowerPoint PPTX	application/vnd.openxmlformats-
	officedocument.presentationml.presentation
Slack file	application/x-atomist-slack-file+json
TAR archive	application/x-tar
Excel XLS	application/vnd.ms-excel
ZIP archive ZIP	application/zip
Audio	
MID	audio/x-midi
MP3	audio/mpeg
MP4	audio/mp4
WAV	audio/x-wav
Image	
BMP	image/tmp
GIF	image/gif
JPG	image/jpeg
PNG	image/png
TIF	image/t ff
Text	
CSS	text/css
CSV	text/csv
HTML	text/html
ICS	text/calendar
RTF	text/richtext

Examples of file type declarations for common file formats Note: file types prefixed by x- are not IANA.

Those prefixed by vnd. are vendor-specific formats.

Video	
AVI	video/x-msvideo
MOV	video/quicktime
MP4	video/mp4
MPG	video/mpeg

§ 11.6:2 When All Else Fails: Octet Streams and Text Stripping

When a processing tool cannot identify a file, it may flag the file as an exception and discontinue processing its contents, but the greater likelihood is that the tool will treat the unidentifiable file as an octet stream and harvest, or "strip out," whatever text or metadata it can identify within the stream. An octet stream is simply an arbitrary sequence or "stream" of data presumed to be binary data stored as eight-bit bytes, or "octets." So, an octet stream is anything the processor fails to recognize as a known file type.

In e-discovery, the risk of treating a file as an octet stream and stripping identifiable text is that the file's content is likely encoded such that whatever plain text is stripped and indexed doesn't fairly mirror relevant content. However, because some text was stripped, the file may not be flagged as an exception that requires special handling; instead, the processing tool records the file as successfully processed notwithstanding the missing content.

§ 11.7 Data Extraction and Document Filters

If electronically stored information were like paper, you could open each item in its associated program (its native application), review the contents, and decide whether the item is relevant or privileged. But ESI is much different than paper documents in crucial ways:

- ESI collections tend to be exponentially more voluminous than paper collections
- ESI is stored digitally, rendering it unintelligible absent electronic processing
- ESI is electronically searchable, while paper documents require laborious human scrutiny
- ESI is readily culled, filtered, and deduplicated, and is inexpensively stored and transmitted
- ESI and associated metadata change when opened in native applications

These and other differences make it impractical and risky to approach e-discovery via the piecemeal use of native applications as viewers. Search would be inconsistent and slow, and deduplication would be impossible. Too, you'd surrender all the benefits of mass tagging, filtering, and production. Lawyers who learn that native productions are superior to other forms of production may mistakenly conclude that native production suggests use of native applications for review. Absolutely not! Native applications are not suited for e-discovery and shouldn't be used for review. E-discovery review tools are the only way to go.

To secure the greatest benefit of ESI in search, culling, and review, we process ingested files to extract their text, embedded objects, and metadata. In turn, we normalize and tokenize extracted contents, add them to a database, and index them for efficient search. These processing operations promote efficiency but impose penalties in terms of reduced precision and accuracy. It's a tradeoff that demands an informed and purposeful balancing of benefits and costs.

Returning to programmer Ann and her efforts to fashion a new file format, Ann had a free hand in establishing the structural layout of her TaggedyAnn data files because she was also writing the software to read them. The ability to easily edit data is a hall-mark of computing. Programmers design files to be able to grow and shrink without impairing the updating and retrieval of their contents. Files hold text, rich media (like graphics and video), formatting information, configuration instructions, metadata, and more. This disparate content exists as a sequence of hexadecimal characters. Some of it may reside at fixed offset addresses measured in a static number of bytes from the start of the file. But because files must be able to grow and shrink, fixed offset addressing alone won't cut it. Instead, files must supply dynamic directories of their contents or incorporate tags that serve as signposts for navigation.

When navigating files to extract their contents, it's not enough to know where the data starts and ends, you must also know how the data is encoded. Is it ASCII text? Uni-

code? JPEG? Is it a date and time value, or perhaps a bit flag where the numeric value serves to signal a characteristic or configuration to the program?

There are two broad approaches used by processing tools to extract content from files. One is to use the application programming interface (API) of the application that created the file. The other is to turn to a published file specification or reverse engineer the file to determine where the data that is sought to be extracted resides and how it's encoded.

A software API allows client applications (i.e., other software) to make requests or "calls" to the API "server" to obtain specific information and to ask the server to perform specific functions. Much like a restaurant, the client can "order" from a menu of supported API offerings without knowing what goes on in the kitchen, where the client generally isn't welcome to enter. Like a restaurant with off-menu items, the API may support undocumented calls intended for a limited pool of users.

For online data reposing in services like Office 365, Dropbox, or OneDrive, there's little choice but to use an API to get to the data; but for data in local files, using a native application's API is something of a last resort because APIs tend to be slow and constraining. Not all applications offer open APIs, and those that do won't necessarily hand off all data needed for e-discovery. For many years, a leading e-discovery processing tool required purchasers to obtain a "bootleg" copy of the IBM/Lotus Notes mail program because the secure structure of Notes files frustrated efforts to extract messages and attachments by any means but the native API.

An alternative to the native application API is the use of data extraction templates called "document filters." Document filters lay out where content is stored within each file type and how that content is encoded and interpreted. Think of them as an extraction template. Document filters can be based on a published file specification or they can be painstakingly reverse engineered from examples of the data—a terrifically complex process that produces outcomes of questionable accuracy and consistency. Because document filters are challenging to construct and keep up to date for each of the hundreds of file types seen in e-discovery, few e-discovery processors build their own library of document filters. Instead, they turn to a handful of commercial and open-source filters.

The leading commercial collection of document filters is Oracle's Outside In, described by its publisher as "a suite of software development kits (SDKs) that provides developers with a comprehensive solution to extract, normalize, scrub, convert, and view the contents of 600 unstructured file formats." Outside In quietly serves as

Processing in E-Discovery, a Primer

the extraction and viewer engine behind many e-discovery review tools, a fact the sellers of those tools are often reluctant to concede. (But I suppose sellers of the Lexus ES aren't keen to note it shares its engine, chassis, and most parts with the cheaper Toyota Avalon.)

Aspose Pty Ltd, an Australian concern, licenses libraries of commercial APIs, enabling software developers to read and write to things like Word documents, Excel spreadsheets, PowerPoint presentations, PDF files, and multiple e-mail container formats. Aspose tools can both read from and write to the various formats, the latter considerably more challenging.

Hyland Software's Document Filters is another developer's toolkit that facilitates file identification and content extraction for more than five hundred file formats, as well as support for OCR, redaction, and image rendering. Per Hyland's website, its extraction tools power e-discovery products from Catalyst and Reveal Software.

A fourth commercial product that lies at the heart of several e-discovery and computer forensic tools (e.g., Relativity, LAW, Ringtail a.k.a. Nuix Discover, and Access Data's FTK) is dtSearch, which serves as both content extractor and indexing engine.

On the open-source side, Apache's Tika is a free toolkit for extracting text and metadata from over a thousand file types, including most file types encountered in e-discovery. Tika was a subproject of the open-source Apache Lucene project, Lucene being an indexing and search tool at the core of several commercial e-discovery tools.

Beyond these five toolsets, the wellspring of document filters and text extractors starts to dry up, which means a broad swath of commercial e-discovery tools relies on a tiny complement of text and metadata extraction tools to build their indexes and front-end their advanced analytics.

In fact, most e-discovery tools in the last fifteen years are proprietary wrappers around code borrowed or licensed from common sources for file identifiers, text extractors, OCR, normalizers, indexers, viewers, image generators, and databases. Bolting these off-the-shelf parts together to deliver an efficient workflow and user-friendly interface is no mean feat.

But as we admire the winsome wrappers, we must remember that these products share the same DNA despite marketing efforts suggesting "secret sauces" and differentiation. More to the point, products built on the same text and metadata extractor share the same limitations and vulnerabilities as that extractor.

§ 11.8 Recursion and Embedded Object Extraction

Just as an essential task in processing is to correctly identify content and apply the right decoding schema, a processing tool must extract and account for all the components of a file that carry potentially responsive information.

Modern productivity files like Microsoft Office documents are rich, layered containers called "compound files." Objects like images and the contents of other file formats may be embedded and linked within a compound file. Think of an Excel spreadsheet appearing as a diagram within a Word document. Microsoft promulgated a mechanism supporting this functionality called "OLE" (pronounced "o-lay" and short for object linking and embedding). OLE supports the ability to drag and drop content between applications and the dynamic updating of embedded content, so the Excel spreadsheet embedded in a Word document, for example, updates to reflect changes in the source spreadsheet file. A processing tool must be able to recognize an OLE object and extract and enumerate all of the embedded and linked content.

A MIME e-mail is also a compound document to the extent that it transmits multipart content, particularly encoded attachments. A processing tool must account for and extract every item in the e-mail's informational payload, recognizing that such content may nest like a Russian doll. An e-mail attachment could be a ZIP container holding multiple Outlook PST mail containers holding e-mail collections that, in turn, hold attachments of OLE documents and other ZIP containers! The mechanism by which a processing tool explores, identifies, unpacks, and extracts all embedded content from a file is called "recursion." It's crucial that a data extraction tool be able to recurse through a file and loop itself to extract embedded content until there is nothing else to be found.

Tika, the open source extraction toolset, classifies file structures in the following ways for metadata extraction:

- simple
- structured
- compound
- simple container
- container with text

§ 11.8:1 Simple Document

A simple document is a single document contained in a single file. Some examples of simple documents include text files and XML files. Any metadata associated with a simple document is for the entire document.

§ 11.8:2 Structured Document

Like simple documents, structured documents are single documents in single files. What makes a structured document different is that the document has internal structure, and there is metadata associated with specific parts of a document. For example, a PDF document has an internal structure for representing each page of the PDF, and there may be metadata associated with individual pages.

§ 11.8:3 Compound Document

A compound document is a single document made up of many separate files, usually stored inside of a single container. Examples of compound documents are DOC (several named streams inside of an OLE file) and XLSX (several named XML files inside of a ZIP file).

§ 11.8:4 Simple Container

A simple container is a container file that contains other files. The container itself does not contain text, but instead contains files that could be any document type. Examples of a simple container include ZIP, tar, tar.gz, and tar.bz2.

§ 11.8:5 Container with Text

Some container files have text of their own and also contain other files. Examples include an e-mail with attachments and a DOC with embedded spreadsheets.

§ 11.9 Family Tracking and Unitization: Keeping Up with Parts

As a processing tool unpacks the embedded components of compound and container files, it must update the database with information about what data came from what file, a relationship called "unitization." In the context of e-mail, recording the relationship between a transmitting message and its attachments is called "family tracking." The transmitting message is the parent object and the attachments are child objects. The processing tool must identify and preserve metadata values applicable to the entire contents of the compound or container file (like system metadata for the parent object) and embedded metadata applicable to each child object. One of the most important metadata values to preserve and pair with each object is the object's custodian or source. After processing, every item in an e-discovery collection must be capable of being tied back to an originating file at time of ingestion, including its prior unitization and any parent-child relationship to other objects.

§ 11.10 Exceptions Reporting: Keeping Track of Failures

It's rare that a sizable collection of data will process flawlessly. There will almost always be encrypted files that cannot be read, corrupt files, files in unrecognized formats or languages, and files requiring optical character recognition (OCR) to extract text. Many documents are not amenable to text search without special handling. Common examples of non-searchable documents are faxes and scans, as well as TIFF images and PDF documents lacking a text layer. A processing tool must track all exceptions and be capable of generating an exceptions report to enable counsel and others with oversight responsibility to rectify exceptions by, for example, securing passwords, repairing or replacing corrupt files, and running OCR against the files. Exceptions resolution is key to a defensible e-discovery process.

Counsel and others who process ESI in discovery should broadly understand the exceptions when handling characteristics of their processing tools and be competent to make necessary disclosures and answer questions about exceptions reporting and resolution. Exceptions are exclusions—the evidence is missing, so exceptions should be disclosed and must be defended. As noted earlier, it's particularly perilous when a processing tool defaults to text stripping in an unrecognized or misrecognized file because the tool may fail to flag a text-stripped file as an exception, requiring resolution. Just because a tool succeeds in stripping some text from a file doesn't mean that all discoverable content was extracted.

§ 11.11 Lexical Preprocessing of Extracted Text

Computers are excruciatingly literal. Computers cannot read. Computers cannot understand language in the way humans do. Instead, computers apply rules assigned by programmers to normalize, tokenize, and segment natural language, all of which are instances of lexical preprocessing—steps to prepare text to be parsed by other tools.

§11.11:1 Normalization

ESI is numbers, and numbers are precise. Variations in those numbers, however subtle to humans, hinder a computer's ability to equate information as humans do. Before a machine can distinguish words or build an index, the streams of text spit out by the document filters must be altered to ultimately increase recall; that is, to ensure that more documents are retrieved by search, even the documents we seek that don't exactly match our queries.

Variations in characters that human beings readily overlook pose big challenges to machines. So, we seek to minimize the impact of these variations through normalization. How we normalize data, and even the order in which steps occur, affects our ability to query the data and return correct results.

§ 11.11:2 Character Normalization

Consider three characteristics of characters that demand normalization: Unicode equivalency, diacriticals (accents), and case (capitalization).

Unicode Normalization: In our discussion of ASCII encoding, we established that each ASCII character has an assigned corresponding numeric value (e.g., a capital "E" is 0100 0101 in binary, "69" in decimal, and "Ox45" in hexadecimal). But linguistically identical characters encoded in Unicode may be represented by different numeric values by virtue of accented letters that have both precomposed and composite references. This means that you can encode specific to the accented letter (a "precomposed character") or you can fashion the character as a composite by pairing the encoding for the base letter with the encoding for the diacritical. For example, the Latin capital "E" with an acute accent (É) may be encoded as either U+00C9 (a precomposed Latin capital letter E with acute accent) or as U+0045 (Latin capital letter E) plus U+0301 (combining acute accent). Both will appear as "É."

Surely when searching in e-discovery we don't want to have to account for every variation in which a character can be encoded in Unicode! To obviate that burden, the Unicode Consortium promulgates normalization algorithms that produce a consistent (normalized) encoding for each identical character. One version of the algorithm reduces all identical characters to a composed version, and another reduces all to a decomposed (composite) version. In e-discovery, we often seek to strip accents so we see more of the latter.

§ 11.11

Diacritical Normalization: Unicode normalization serves to ensure that the same canonical character is encoded in a consistent way. But often—especially in the United States—we want accented characters to be searchable whether a diacritical is employed or not. This requires normalizing the data to forge a false equivalency between accented characters and their non-accented ASCII counterparts. For instance, if you search for "resume" or "cafe," you will pick up instances of "resumé" and "café." As well, we must normalize ligatures like the German Eszett (ß) seen in the word "straße," or "street."

The major processing tools offer filters that convert alphabetic, numeric, and symbolic Unicode characters not in the first 127 ASCII characters (the "Basic Latin" Unicode block) into their reasonable ASCII equivalents, if any. Lucene and Elasticsearch offer "ASCIIFolding" filters for this. dtSearch strips diacritics by default when it creates an index, but indexes can optionally be made accent-sensitive by re-indexing.

Case Normalization: The Latin alphabet is bicameral, meaning it employs uppercase and lowercase letters to enhance meaning. (The terms "uppercase" and "lowercase" derive from the customary juxtaposition of the shallow drawers, or "cases," that held movable type for printing presses.) By contrast, languages such as Chinese, Arabic, and Hebrew are unicameral and use no capitalization. Because people capitalize indiscriminately—particularly in e-mail and messaging—most often we want search queries to be case-insensitive such that "DOE," "Doe," and "doe" all return the same hits. Other times the ability to limit a search to a case-specific query is advantageous, such as by searching just "DOE" when interested in the Department of Energy and when search precision is more important than recall.

Just as processing tools can be configured to "fold" Unicode characters to ASCII equivalents, they can fold all letters to their uppercase or lowercase counterparts, rendering an index that is case-insensitive. Customarily, the normalization of case will require the specification of a default language because of different capitalization conventions attendant to diverse cultures.

§ 11.11:3 Impact of Normalization on Discovery Outcomes

Although all processing tools draw on a handful of filters and algorithms for the aforementioned and other normalization processes, not all processors implement normalization in the same sequence or with identical default settings. Accordingly, it's routine to see tools produce varying outcomes in culling and search because of differences in character normalization. Whether these differences are material or not

depends on the nature of the data and the inquiry, but any service provider and case manager should know how their tool of choice normalizes data.

In the sweep of a multimillion-document project, the impact of normalization might seem trivial. Yet character normalization affects the whole collection and plays an outsize role in what's filtered and found. It's an apt reminder that a good working knowledge of processing equips e-discovery professionals to "normalize" *expectations*, especially expectations as to what data will be seen and searchable going forward. The most advanced techniques in analytics and artificial intelligence are no better than what emerges from processing. If the processing is off, it's akin to fancy joinery applied to rotten wood.

Lawyers must fight for quality before review. Sure, review is the part of e-discovery most lawyers see and understand, and therefore the part many fixate on. As well, review is the costliest component of e-discovery and the one with cool tools. But here's the bottom line: the most sophisticated MRI scanner won't save those who don't survive the trip to the hospital. It's more important to have triage that gets people to the hospital alive than the best-equipped emergency room. Collection and processing are the EMTs of e-discovery. If we don't pay close attention to quality, completeness, and process before review, review won't save us.

§ 11.12 Time Zone Normalization

You needn't be an Einstein of e-discovery to appreciate that time is relative. When parsing a message thread, it's common to see e-mails from Europe to the U.S. prompt replies that, at least according to embedded metadata, appear to precede by hours the messages they answer. Time zones and daylight saving time both work to make it difficult to correctly order documents and communications on a consistent timeline. A common processing task is to normalize date and time values according to a single temporal baseline, often Coordinated Universal Time (UTC)—essentially Greenwich Mean Time—or to any other time zone the parties choose. The differential between the source time and UTC offset may then be expressed as plus or minus the numbers of hours separating the two (e.g., "UTC-0500" to denote five hours earlier than UTC).

§ 11.13 Parsing and Tokenization

To this point, we've focused on efforts to identify a file's format, then extract its content and metadata—important tasks, because if you don't get the file's content out and properly decoded, there's nearly nothing to work with. But getting data out is just the first step. Now we must distill the extracted content into the linguistic components that serve to convey the file's informational payload; that is, we need to isolate the words within the documents and construct an index of those words to allow us to instantly identify or exclude files based on their lexical content.

There's a saying that anything a human being can do after age five is easy for a computer, but mastering skills humans acquire earlier is hard. Calculate pi to 31 trillion digits? Done! Read a Dr. Seuss book? Sorry, no can do.

Humans are good at spotting linguistic units like words and sentences from an early age, but computers must identify lexical units or "tokens" within extracted and normalized character strings, a process called "tokenization." When machines search collections of documents and data for keywords, they don't search the extracted text of the documents or data for matches; instead, they consult an index of words built from extracted text. Machines cannot read; instead, computers identify "words" in documents because their appearance and juxtaposition meet certain tokenization rules. These rules aren't uniform across systems or software. Many indexes simply don't index short words (e.g., two-letter words, acronyms, and initializations), and none index single letters or numbers.

Tokenization rules also govern such things as the handling of punctuated terms (as in a compound word like "wind-driven"), capitalization/case (will a search for "roof" also find "Roof"?), diacritical marks (will a search for "Rene" also find "René"?), and numbers and single letters (will a search for "Clause 4.3" work? What about a search for "Plan B"?). Most people simply assume these searches will work. Yet in many e-discovery search tools, they don't work as expected or don't work at all.

So, how do you train a computer to spot sentences and words? What makes a word a word and a sentence a sentence?

Languages derived from Latin-, Cyrillic-, or Greek-based writing systems, such as English and some European languages, are "segmented;" that is, they tend to set off ("delimit") words by white space and punctuation. Consequently, most tokenizers for segmented languages base token boundaries on spacing and punctuation. This seems like a simple solution at first blush, but one complicated by hyphenated words, contractions, dates, phone numbers, and abbreviations. How does the machine distinguish a word-break hyphen from a true or lexical hyphen? How does the machine distinguish the periods in the salutation "Mr." or the initialization "G.D.P.R." from periods that signal the ends of sentences? In the realm of medicine and pharmacology, many words contain numbers, dashes, and parentheses as integral parts. How could you defend a search for ibuprofen if you failed to also seek instances of (RS)-2-(4-(2-methylpropyl)phenyl)propanoic acid?

Again, tokenization rules aren't uniform across systems, software, or languages. Some tools are simply incapable of indexing and searching certain characters. These exclusions impact discovery in material ways. Several years ago, after contentious motion practice, a court ordered the parties to search a dataset using queries incorporating the term "20%." No one was pleased to learn their e-discovery tools were incapable of searching for the percent sign.

You cannot run a query in Relativity that includes the percentage sign (%) because Relativity uses dtSearch as an indexing tool, and dtSearch has reserved the character "%" for another purpose. This is true no matter how you tweak the settings because "%" simply cannot be added to the index and made searchable.³ When you run a search, you won't be warned that the search is impossible, you'll simply get no hits on any query searching for the percent sign.

Using dtSearch/Relativity as another example, you can specify the way to process hyphens at the time an index is created, but you cannot change how hyphens are handled without re-indexing the collection. The default setting is to treat hyphens as spaces, but there are four alternative treatments that the dtSearch engine supports for the treatment of hyphens when indexing documents: spaces, searchable text, ignored, and "all three." See table below.

For most applications, treating hyphens as spaces is the best option. Hyphens are translated to spaces during indexing and during searches. For example, if you index "first-class mail" and search for "first class mail," "first-class-mail," or "first-class mail," you will find the phrase correctly.

HyphenSettings Value	Meaning	
dtsoHyphenAsIgnore	index "first-class" as "firstclass"	
dtsoHyphenAsHyphen	index "first-class" as "first-class"	

Hyphen values in dtSearch

^{3.} There's a clumsy workaround to this described in the Help section of Relativity's website: https://help.relativity.com/9.2/RelativityOne'Content/Recipes/Searching_Filtering_and_Sorting/Searching_for_symbols.htm; however, it doesn't serve to make a percentage value searchable so much as permit a user to find a numeric value followed by any symbol. For example, you'd hit with 75%, but also 75! and 75#. Even this kludge requires rebuilding all indexes.

HyphenSettings Value	Meaning	
dtsoHyphenAsSpace	index "first-class" as "first" and "class"	
dtsoHyphenAll	index "first-class" all three ways	

Hyphen values in dtSearch

The "all three" option has one advantage over treating hyphens as spaces: it will return a document containing "first-class" in a search for "firstclass." Otherwise it provides no benefit over treating hyphens as spaces and also has some significant disadvantages: the "all three" option generates many extra words during indexing. For each pair of words separated by a hyphen, six words are generated in the index, and if hyphens are treated as significant at search time, the index can produce unexpected results in searches involving longer phrases or words with multiple hyphens.

By default, dtSearch and Relativity treat all the following characters as spaces: ! " # & '() * +, . / :; < = > ? @ [\5 c]^` {|} ~

Although several of the characters above can be made searchable by altering the default setting and re-indexing the collection, the following characters *cannot* be made searchable in dtSearch and Relativity: () * ? % @ $\sim \& :=$

Stop Words: Some common "stop words" or "noise words" are excluded from an index when it's compiled. E-discovery tools typically exclude dozens or hundreds of stop words from indexes. The table below lists 123 English stop words excluded by default in dtSearch and Relativity:

Begins with	Stop words	
A	about, after, all, also, another, any, are, as, at	
В	be, because, been, before, being, between, but, both, by	
С	came, can, come, could	
D	did, do, does	
Е	each, else	
F	for, from	
G	get, got	
Н	has, had, he, have, her, here, him, himself, his, how	
Ι	if, in, into, is, it, its	

Common stop words

Begins with	Stop words
J	just
L	like
М	make, many, me, might, more, most, much, must, my
N	never, no, now
0	of, on, only, other, our, out
S	said, same, see, should, since, so, some, still, such
Т	take, than, that, the, their, them, then, there, these, they, this, those, through, to, too
U	under, up, use
V	very
W	want, was, way, we, well, were, what, when, where, which, while, who, will, with, would
Y	you, your

Common stop words

Source: Relativity website (accessed November 3, 2019).

Relativity won't index punctuation marks, single letters or numbers. Nuix Discovery (formerly Ringtail) uses a similar English stop word list, except Nuix indexes the words "between," "does," "else," "from," "his," "make," "no," "so," "to," "use," "want," and "does" where Relativity won't. Relativity indexes the words "an," "even," "further," "furthermore," "hi," "however," "indeed," "made," "moreover," "not," "or," "over," "she," and "thus" where Nuix won't. Does it make sense that both tools exclude "he" and "her," and both include "hers," but only Relativity excludes "his?"

Tools built on the open-source Natural Language Toolkit won't index 179 English stop words. In other products, I've seer, between five hundred and seven hundred English stop words excluded. In one notorious instance, the two words that made up the company's own name were both stop words in their e-discovery system—they literally could not find their own name or other stop words in queries they'd agreed to run!

Remember, *if it's not indexed, it's not searched*. Putting a query in quotes won't make any difference. No warning messages appear when you run a query including stop words, so it's the obligation of those running searches to acknowledge the incapability of the search. "No hits" is not the same thing as "no documents." If a party or counsel knows that the systems or searches used in e-discovery will fail to perform as expected, they should affirmatively disclose such shortcomings. If a party or counsel is uncertain whether systems or searches work as expected, they should find out by, for example, running tests to be reasonably certain.

No system is perfect, and perfect isn't the e-discovery standard. Often, we must adapt to the limitations of systems or software. But we must know what a system can't do before we can find ways to work around its limitations or set expectations consistent with actual capabilities, not magical thinking and unfounded expectations.

§ 11.14 Building a Database and Concordance Index

This primer is about processing, and the database (and viewer) belong to the realm of review tools and their features. However, a brief consideration of their interrelation-ship is useful.

§ 11.14:1 Database

At every step of processing, information derived from and about the items processed is continually handed off to a database. As the system ingests each file, a record of its name, size, and system metadata values becomes part of the database. Sources called "custodians" when they are individuals—are identified and comprise database fields. The processor calculates hash values and contributes them to the database. The tool identifies and extracts application metadata values from the processed information items, including authoring data for documents as well as subject, sender, and recipient data for e-mail messages, among other things. The database is where items are enumerated, that is, assigned an item number that will uniquely identify each item in the processed collection. This is an identifier distinct from any Bates numbers subsequently assigned to items when produced.

The database lies at the heart of all e-discovery review tools. It's the recipient of much of the information derived from processing. But note that the database is *not* the index of text extracted from the processed items. The concordance index, the database, and a third component, the document viewer, operate in such a tightly coupled manner that they seem like one.

A query of the index customarily triggers a return of information from the database about items "hit" by the query, and the contents of those items are, in turn, depicted in the viewer, often with hits highlighted. The perceived quality of commercial e-discovery review tools is a function of how seamlessly and efficiently these discrete functional components integrate to form a robust and intuitive user interface and experience.

Much like the file identification and content extraction tools discussed, e-discovery tool developers tend not to code databases from scratch, but instead build atop a handful of open source or commercial database platforms. Notable examples are SQL Server and SQLite. Notwithstanding Herculean efforts by marketers to suggest differences, e-discovery tools tend to share the same or similar "database DNA." Users are none the wiser to the common foundations because the "back end" of discovery tools (the program's code and database operations layer) tends to be hidden from users and wrapped in an attractive interface.

§ 11.14:2 Concordance Index

Though there was a venerable commercial discovery tool called Concordance (now Cloudnine), the small-c term "concordance" describes an alphabetical listing, particularly a mapping, of the important words in a text. Historically, scholars spent years painstakingly constructing concordances (or "full-text" indexes) of Shakespeare's works or the Bible by hand. In e-discovery, software builds concordance indexes to speed up lexical search. While it's technically feasible to keyword search all documents in a collection one after another (a so-called "serial search"), it's terribly inefficient.⁴

Instead, the universal practice in e-discovery is to employ software to extract the text from information items, tokenize the contents to identify words, and then construct a list of each token's associated document and location. Accordingly, text searches in ediscovery don't search the evidence, they only search a concordance index of tokenized text. This is a crucial distinction because it means the quality of search in e-discovery is only as effective as the index is complete.

"Indexing" is when data is processed to form a highly efficient cross-reference lookup to facilitate rapid searching. Notable examples of concordance indexing tools are dtSearch, MarkLogic, Hyland Enterprise Search, Apache Lucene along with the Lucene-related products, Apache SOLR, and Elasticsearch.

^{4.} Computer forensic examiners still use serial searches when the corpus is modest and when employing global regular expression and print (GREP) searches to identify patterns conforming to, for example, social security or credit card numbers.

Lucene is an open-source, inverted, full-text index. It takes the tokenized and normalized word data from the processing engine and constructs an index for each token (word). It's termed an "inverted index" because it inverts a page-centric data structure (page to words) to a keyword-centric data structure (words to pages).

The full-text index consists of a token identifier (the word), a listing of documents containing the token, and the position of the token within those documents (offset start- and end-positions, plus the increment between tokens). See figure below. Querying the index returns a listing of tokens and positions for each. It may also supply an algorithmic ranking of the results. Multiword queries return a listing of documents where there's an intersection of the returns for each token searched and found.



An advantage of tools like Lucene is its ability to be updated incrementally (i.e., new documents can be added without the need to recreate a single, large index).

§ 11.15 Culling and Selecting Dataset

Processing is not an end but a means by which potentially responsive information is exposed, enumerated, normalized, and passed on for search, review, and production. Although much culling and selection occurs in the search and review phase, the processing phase is an opportunity to reduce data volumes by culling and selecting by defensible criteria.

Now that the metadata is in a database and the collection has been made text-searchable by the creation of a concordance index, it's feasible to filter the collection by, for example, date ranges, file types, Internet domains, file size, custodian, and other objective characteristics. We can also cull the dataset by immaterial item suppression, de-NISTing, and deduplication, all discussed below.

The crudest but most common culling method is keyword and query filtering; that is, lexical search. Lexical search and its shortcomings are beyond the scope of this processing primer, but it should be clear by now that the quality of the processing bears

materially on the ability to find what we seek through lexical search. No search and review process can assess the content of items missed or malformed in processing.

§ 11.15:1 De-NISTing

De-NISTing is a technique used in e-discovery and computer forensics to reduce the number of files requiring review by excluding standard components of the computer's operating system and off-the-shelf software applications like Word, Excel, and other parts of Microsoft Office. Everyone has this digital detritus on their systems—things like Windows screen saver images, document templates, clip art, system sound files, and so forth. It's the stuff that comes straight off the installation disks, and it's just noise to a document review.

Eliminating this noise is called "de-NISTing" because those noise files are identified by matching their cryptographic hash values (i.e., digital fingerprints—explanation to follow) to a huge list of software hash values maintained and published by the National Software Reference Library, a branch of the National Institute for Standards and Technology (NIST). The NIST list is free to download, and pretty much everyone who processes data for e-discovery and computer forensic examination uses it.

The value of de-NISTing varies according to the makeup of the collection. It's very effective when ESI has been collected indiscriminately or by forensic imaging entire hard drives (including the operating system and executable files). De-NISTing is of limited value when the collection is composed primarily of user-created files and messages as distinguished from system files and executable applications. As a rule, the better focused the e-discovery collection effort (i.e., the more targeted the collection), the smaller the volume of data culled via de-NISTing.

§ 11.15:2 Cryptographic Hashing

Because ESI is just a bunch of numbers, we can use algorithms (mathematical formulas) to distill and compare those numbers. Every student of electronic discovery learns about cryptographic hash functions and their usefulness as tools to digitally fingerprint files in support of identification, authentication, exclusion, and deduplication. When I teach law students about hashing, I tell them that hash functions are published, standard mathematical algorithms into which we input digital data of arbitrary size from which the hash algorithm spits out a bit string (again, just a sequence of numbers) of fixed length called a "hash value." Hash values almost exclusively correspond to the digital data fed into the algorithm (termed "the message") such that the chance of two different messages sharing the same hash value (called a "hash collision") is exceptionally remote. But because it's possible, we can't say each hash value is truly unique.

Using hash algorithms, any volume of data—from the tiniest file to the contents of entire hard drives and beyond—can be almost uniquely expressed as an alphanumeric sequence. In the case of the MD5 hash function, data is distilled to a value written as 32 hexadecimal characters (0–9 and A–F). It's hard to understand until you've figured out Base16, but those 32 characters represent 340 trillion trillion trillion different possible values (2¹²⁸ or 16³²).

Hash functions are one-way calculations, meaning you can't reverse ("invert") a hash value and ascertain the data corresponding to the hash value in the same way that you can't decode a human fingerprint to deduce an individual's eye color or IQ. It identifies, but it doesn't reveal. Another key feature of hashing is that, due to the so-called "avalanche effect" characteristic of a well-constructed cryptographic algorithm, when the data input changes even slightly, the hash value changes dramatically, meaning there's no discernable relationship between inputs and outputs. Similarity between hash values doesn't signal any similarity in the data hashed.

There are many different hash algorithms, and different hash algorithms generate different hash values for the same data; that is, the hash value for the phrase "Mary had a little lamb" will be the following in each of the following hash algorithms:

- MD5: e946adb45d4299def2071880d30136d4
- SHA-1: bac9388d0498fb378e528d35abd05792291af182
- SHA-256: efe473564cb63a7bf025dd691ef0ae0ac906c03ab408375b9094e326c2a d9a76

It's identical data, but it prompts different hashes using different algorithms. Conversely, identical data will generate identical hash values when using the same hash function. Freely published hash functions are available to all, so if two people (or machines) anywhere use the same hash function against data and generate matching hash values, their data is identical. If they get different hash values, they can be confident the data is different. The differences may be trivial in practical terms, but any difference is sufficient to produce markedly different hash values.

§ 11.15:3 Deduplication

Processing information items in order to calculate hash values supports several capabilities, but probably none more useful than deduplication.

Near-Deduplication: A modern hard drive holds trillions of bytes, and even a single Outlook e-mail container file typically comprises billions of bytes. Accordingly, it's easier and faster to compare 32-character/16-byte "fingerprints" of voluminous data than to compare the data itself, particularly as the comparisons must be made repeatedly when information is collected and processed in e-discovery. In practice, each file ingested and item extracted is hashed, and its hash value is compared to the hash values of items previously ingested and extracted to determine if the file or item has been seen before. The first file is sometimes called the "pivot file," and subsequent files with matching hashes are suppressed as duplicates, and the instances of each duplicate and certain metadata is typically noted in a deduplication or "occurrence" log.

When the data is comprised of loose files and attachments, a hash algorithm tends to be applied to the full contents of the files. Notice that I said "contents." Some data we associate with files is not actually stored inside the file but must be gathered from the file system of the device storing the data. Such "system metadata" is not contained within the file and, thus, is not included in the calculation when the file's content is hashed. A file's name is perhaps the best example of this. Recall that even slight differences in files cause them to generate different hash values. But since a file's name is not typically housed within the file, it can be changed without altering its hash value.

The ability of hash algorithms to deduplicate depends upon whether the numeric values that serve as building blocks for the data differ from file to file. Keep that firmly in mind as we consider the many forms that the informational payload of a document may manifest.

A Word DOCX document is constructed of a mix of text and rich media encoded in Extensible Markup Language (XML) then compressed using the ubiquitous ZIP compression algorithm. It's a file designed to be read by Microsoft Word.

When you print the "same" Word dccument to an Adobe PDF format, it's reconstructed in a page description language specifically designed to work with Adobe Acrobat. It's structured, encoded, and compressed in an entirely different way than the Word file and, as a different format, carries a different binary header signature, too. When you take the printed version of the document and scan it to a Tagged Image File Format (TIFF), you've taken a picture of the document now constructed in yet another different format—one designed for TIFF viewer applications. To the uninitiated, the two versions are all the "same" document and might look pretty much the same printed to paper, but as ESI, their structures and encoding schemes are radically different. Moreover, even files generated in the same format may not be digitally identical when made at separate times. For example, no two optical scans of a document will produce identical hash values because there will always be some variation in the data acquired from scan to scan. Slight differences, perhaps, but any difference at all in content is going to frustrate the ability to generate matching hash values.

Opinions are cheap. Testing is truth. To illustrate this, I created a Word document of the text of Lincoln's Gettysburg Address. First, I saved it in the latest DOCX Word format. Then I saved a copy in the older DOC format. Next, I saved the Word document to a PDF format, using both the Save as PDF and Print to PDF methods. Finally, I printed the document and scanned to TIFF and PDF. Without shifting the document on the scanner, I scanned it several times at matching and differing resolutions.

I then hashed all the iterations of the "same" document. As the table below demonstrates, none of them matched hash-wise, not even the successive scans of the paper document:

FILENAME	MD5 HASH	FILE SIZE
GBA.docx	5074fbb210ed4e9e498e4908a946a871	21Kb
GBA.doc	1aacf60b523eb8cf2829208ffee58005	26Kb
GBA-Save as.pdf	c8d68e84ea573772d14dc536fbe8594e	83Kb
GBA-Word generated.pdf	2be09d776682fee46c79be8ecac03ec5	27Kb
GBA-scan1.tiff	0f5fdbbcbc96abc05b43f356c4e24818	967Kb
GBA-scan2.tiff	04c93ac7eb6716bc96bc3a396fed882a	967Kb
GBA-scan3_600BW.tiff	93e726efa56fe7f25956da6664a32957	1,060Kb
GBA-scan4_600BW.tiff	8d97df97c28414d4b61bb8b88b1db343	1,060Kb
GBA_scan5_300GS.pdf	b558eccee1bdcc5f26de53763f89aef4	2,950Kb
GBA scan6 300GS.pdf	520be78a7ec81ebebece5a19e9c6e425	2,930Kb

Table: Document hash values

Thus, file hash matching—the simplest and most defensible approach to deduplication—won't serve to deduplicate the "same" document when it takes different forms or is made optically at separate times. Now here's where it can get confusing. If you copied any of the electronic files listed above, the duplicate files would hash match the source originals and would handily deduplicate by hash. Consequently, multiple copies of the same electronic files will deduplicate, but this is because the files being compared have the same digital content. But we must be careful to distinguish the identicality seen in multiple iterations of the same file from the pronounced differences seen when we generate different electronic versions at different times from the same content. One notable exception seen in my testing was that successively saving the same Word document to PDF format in the same manner sometimes generated identical PDF files. It didn't occur consistently (i.e., if enough time passed, changes in metadata in the source document triggered differences, prompting the calculation of different hash values), but it happened, so it is worth mentioning.

Consider hash matching in this real-life scenario: The source data was Outlook PSTs from various custodians, each under two gigabytes in size. The form of production was single messages as MSGs. Reportedly, the new review platform (actually a rather old concept search tool) was incapable of accepting an overlay load file that could simply tag the items already produced, so the messages already produced would have to be culled from the PSTs before they were loaded. Screwy, to be sure, but we take our cases as they come, right?

It's important to know that a somewhat obscure quirk of the MSG message format is that when the same Outlook message is exported as an MSG at various times, each exported message generates a different hash value because of embedded time-of-creation values. The differing hash values make it impossible to use hashes of MSGs for deduplication without processing (i.e., normalizing) the data to a format better suited to the task.

Here, a quick primer on deduplication of e-mail might be useful. Mechanized deduplication of e-mail data can be grounded on three basic approaches:

1. Hashing the entire message as a file (i.e., a defined block of data) that contains the e-mail messages and then comparing the resulting hash value for each individual message file. If they match, the files hold the same data. This tends not to work for e-mail messages exported as files because when an e-mail message is stored as a file, messages that we regard as identical in common parlance (such as identical message bodies sent to multiple recipients) are not identical in terms of their byte content. The differences tend to reflect either variations in transmission, seen in the message header data (the messages having traversed different paths to reach different recipients), or variations in time (the same message containing embedded time data when exported to single message storage formats as discussed above, with respect to the MSG format).

- 2. Hashing segments of the message using the same hash algorithm and comparing the hash values for each corresponding segment to determine relative identicality. With this approach, a hash value is calculated for the various parts of a message (e.g., Subject, To, From, CC, message body, and attachments), and these values are compared to the hash values calculated against corresponding parts of other messages to determine if they match. This method requires exclusion of parts of a message that are certain to differ (such as portions of message headers containing server paths and unique message IDs) and normalization of segments so that contents of those segments are presented to the hash algorithm in a consistent way.
- 3. Textual comparison of segments of the message to determine if certain segments of the message match to such an extent that the messages may be deemed sufficiently "identical" so they can be treated as the same for purposes of review and exclusion. This is much the same as approach 2. above, but without the use of hashing that compares the segments.

Arguably, a fourth approach entails a mix of these methods.

All of these approaches can be frustrated by working from differing forms of the "same" data because, from the standpoint of the tools that compare the information, the forms are significantly different. Thus, if a message has been "printed" to a TIFF image, the bytes that make up the TIFF image bear no digital resemblance to the bytes comprising the corresponding e-mail message any more than a photo of a rose smells or feels like the rose.

In short, changing forms of ESI changes data, and changing data changes hash values. Deduplication by hashing requires the same source data and the same consistent application of algorithms. This is easy and inexpensive to accomplish, but it requires a compatible workflow to ensure that evidence is not altered during processing so as to prevent the application of simple and inexpensive mechanized deduplication.

When parties cannot deduplicate e-mail, the reasons will likely be one or more of the following:

1. They are working from different forms of the ESI

- 2. They are failing to consistently exclude inherently non-identical data (like message headers and IDs) from the hash calculation
- 3. They are not properly normalizing the message data (such as by ordering all addresses alphabetically without aliases)
- 4. They are using different hash algorithms
- 5. They are not preserving the hash values throughout the process
- 6. They are changing the data

The excerpts that follow are from Microsoft and Relativity support publications, each describing the methodology employed to deduplicate e-mail messages.

Office 365 Deduplication: Office 365 eDiscovery tools use a combination of the following e-mail properties to determine whether a message is a duplicate.⁵

- InternetMessageId: This property specifies the Internet message identifier of an e-mail message, which is a globally unique identifier that refers to a specific version of a specific message. This ID is generated by the sender's e-mail client program or the host e-mail system that sends the message. If a person sends a message to more than one recipient, the Internet message ID will be the same for each instance of the message. Subsequent revisions to the original message will have a different message identifier.
- *ConversationTopic:* This property specifies the subject of the conversation thread of a message. The value of the ConversationTopic property is the string that describes the overall topic of the conversation. A conversation consists of an initial message plus all messages sent in reply to the initial message. Messages within the same conversation have the same value for the ConversationTopic property. The value of this property is typically the subject line from the initial message that spawned the conversation.
- *BodyTagInfo:* This is an internal Exchange store property. The value of this property is calculated by checking various attributes in the body of the message. This property is used to identify differences in the body of messages.

Relativity E-Mail Deduplication: The Relativity Processing Console (RPC) generates four different hashes for e-mails and keeps each hash value separate, which

^{5.} https://docs.microsoft.com/en-us/microsoft-365/compliance/de-duplication-in-ediscovery -search-results.

allows users to deduplicate in the RPC based on individual hashes and not an allinclusive hash string. For example, if you're using the RPC, you have the ability to deduplicate one custodian's files against another's based only on the body hash and not the attachment or recipient hashes. Note that the following information is relevant only to the RPC and not to web processing in Relativity:

- "Body hash" takes the text of the body of the e-mail and generates a hash
- "Header hash" takes the message time, subject, author's name and author's e-mail and generates a hash
- "Recipient hash" takes the recipient's name and e-mails and generates a hash
- "Attachment hash" takes each SHA-256 hash of each attachment and hashes the SHA-256 hashes together

MessageBodyHash: To calculate an e-mail's MessageBodyHash, the RPC-

- 1. Removes all carriage returns, line feeds, spaces, and tabs from the body of the e-mail to account for formatting variations. An example of this is when Outlook changes the formatting of an e-mail and displays a message stating "Extra line breaks in this message were removed."
- 2. Captures the PR_BODY tag from the MSG (if it's present) and converts it into a Unicode string.
- 3. Gets the native body from the PR_RTF_COMPRESSED tag (if the PR_BODY tag isn't present) and either converts the HTML or the RTF to a Unicode string.
- 4. Constructs a SHA-256 hash from the Unicode string derived in step 2 or 3 above.

HeaderHash: To calculate an e-mail's HeaderHash, the RPC-

- 1. Constructs a Unicode string containing Subject<crlf>Sender-Name<crlf>SenderEMail<crlf>ClientSubmitTime.
- 2. Derives the SHA-256 hash from the header string. The ClientSubmitTime is formatted with the following: m/d/yyyy hh:mm:ss AM/PM. The following is an example of a constructed string:

RE: Your last email

Robert Simpson

robert@relativity.com

10/4/2010 05:42:01 PM

RecipientHash: To calculate an e-mail's RecipientHash, the RPC-

- 1. Constructs a Unicode string by looping through each recipient in the e-mail and inserting each recipient into the string. Note that BCC is included in the Recipient's element of the hash.
- 2. Derives the SHA-256 hash from the recipient string Recipient-Name<space>RecipientEMail<crlf>. The following is an example of a constructed recipient string of two recipients:

Russell Scarcella

rscarcella@relativity.com

Kristen Vercellino

kvercellino@relativity.com

AttachmentHash: To calculate an e-mail's AttachmentHash, the RPC-

- 1. Derives a SHA-256 hash for each attachment. If the attachment is a loose file (not an e-mail), then the normal standard SHA-256 file hash is computed for the attachment. If the attachment is an e-mail, the e-mail hashing algorithm described in section 1.2 is used to generate all four deduplication hashes. These hashes are then combined using the algorithm described in section 1.3 to generate a singular SHA-256 attachment hash.
- 2. Encodes the hash in a Unicode string as a string of hexadecimal numbers without <crlf> separators.
- Constructs a SHA-256 hash from the bytes of the composed string in Unicode format. The following is an example of constructed string of two attachments: 80D03318867DB05E40E20CE10B7C8F511B1D0B9F336EF2C787CC3D 51B9E26BC9974C9D2C0EEC0F515C770B8282C87C1E8F957FAF34654 504520A7ADC2E0E23EA

Calculating Relativity deduplication hash: To derive the Relativity deduplication hash, the system—

1. Constructs a string that includes the hashes of all four e-mail components described above.

- 2. Converts that string to a byte array of UTF8 values.
- 3. Feeds the bytes into a standard MD5/SHA-1/SHA-256 subroutine, which then computes the hash of the UTF8 byte array.

Note: If two e-mails or loose files have an identical body, attachment, recipient, and header hash, they are duplicates.⁶

§ 11.16 Other Processing Tasks

This primer addresses the core functions of ESI processing in e-discovery, but there are many other processing tasks that make up today's powerful processing tools.

§ 11.16:1 Foreign Language Detection

Several commercial and open-source processing tools support the ability to recognize and identify foreign language content, enabling selection of the right filters for text extraction, character set selection, and diacritical management. Language detection also facilitates assigning content to native speakers for review.

§ 11.16:2 Entropy Testing

Entropy testing is a statistical method used to identify encrypted files and then flag them for special handling.

§ 11.16:3 Decryption

Some processing tools support the use of customizable password lists to automate decryption of password-protected items when credentials are known.

§ 11.16:4 Bad Extension Flagging

Most processing tools warn of a mismatch between a file's binary signature and its extension. This is potentially useful to resolve exceptions and detect data hiding.

^{6.} https://help.relativity.com/9.2/Content/Relativity/Processing/deduplication_considerations.htm#Technica.

§ 11.16:5 Color Detection

When color conveys information, it's useful to detect such usage and direct colorenhanced items to production formats other than grayscale TIFF imaging.

§ 11.16:6 Hidden Content Flagging

It's common for evidence, especially Microsoft Office content, to incorporate relevant content (like collaborative comments in Word documents and speaker notes in Power-Point) that won't appear in the production set. Flagging such items for special handing is a useful way to avoid missing discoverable (and potentially privileged) content.

§ 11.16:7 N-Gram and Shingle Generation

Increasingly, advanced analytics like predictive coding aid the review process, and they depend on the ability to map document content in ways that support algorithmic analysis. N-gram generation and text shingling are text-sampling techniques that support latent-semantic analytics.

§ 11.16:8 Optical Character Recognition (OCR)

OCR is the primary means by which text stored as imagery—thus lacking a searchable text layer (e.g., TIFF images, JPGs, and PDFs)—can be made text-searchable. Some processing tools natively support OCR, and others require users to run OCR against exception files in a separate workflow and then re-ingest the content accompanied by its OCR text.

§ 11.16:9 Virus Scanning

Files collected in e-discovery may be plagued by malware, so processing may include methods to quarantine afflicted content via virus scanning.

§ 11.17 Production Processing

In this chapter we've concentrated on processing before search and review, but there's typically a processing workflow that follows search and review: "production processing." Some tools and workflows convert items in a collection to imaged formats (TIFF or PDF) before review; in others, imaging is obviated by use of a viewer component of the review tool. If not imaged before review, the e-discovery tool may need to process items that have been selected for production and redaction to imaged formats suited to production and redaction. Further in conjunction with the production process, the tool will generate a load file to transmit extracted metadata and data describing the organization of the production, such as pointers to TIFF images and text extractions. Production processing will also entail assignment of Bates numbers to the items produced as well as the embossing of Bates numbers and restrictive language (i.e., "produced subject to protective order").



Figure 11-3: E-Discovery processing model



Figure 11-4: Anatomy of a Word DOCX file

By changing a Word document's extension from DOCX to ZIP, you can "trick" Windows into decompressing the file and sneak a peek into its internal structure and contents. Those contents little resemble the document you'd see in Word, but as you peruse the various folders and explore their contents you'll find the text, embedded images, formatting instructions, and other components Word assembles to compose the document. The root level of the decompressed file (upper left) contains four folders and one XML file.

§ 11.17

Chapter 12

Privilege Waiver, Rule 502, and Clawback/Sneak Peek Agreements

Kathy Owen Brown, Allison O. Skinner, and Peter S. Vogel

§ 12.1 Introduction: Large Amount of Collected Information Makes Privilege Review Difficult

As electronically stored information ("ESI") has proliferated, the threat of waiver of attorney-client privileged documents or documents subject to the attorney work-product doctrine based on inadvertent disclosure has required time-consuming and expensive page-by-page review of millions of documents. Notwithstanding this effort, privileged documents still slip through even exhaustive review. *Pacific Coast Steel v. Leany*, No. 2:09-cv-02190-KJD-PAL. 2011 WL 4704217, at *5 (D. Nev. Oct. 4, 2011); *Coburn Group, LLC v. Whitecap Advisors, LLC*, 640 F. Supp. 2d 1032, 1040 (N.D. Ill. 2009); *see Rhoads Indus., Inc. v. Bldg. Materials Corp. of America*, 254 F.R.D. 216, 220 (E.D. Pa. 2008). In both *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 257 (D. Md. 2008) and *Hopson v. Mayor & City Council of Baltimore*, 232 F.R.D. 228, 235–36 (D. Md. 2005), Judge Paul Grimm analyzed the problems with "'old world' record-by-record pre-production privilege review" in modern electronic discovery, including inevitable lengthening of pretrial discovery and disproportionate discovery costs in relation to the claimed damages. *See Hopson*, 232 F.R.D. at 243–44; *Victor Stanley*, 250 F.R.D. at 259 n.5, n.7.

This chapter will focus on how a party may avoid any claim of waiver of privilege based on the inadvertent disclosure of privileged documents. This chapter will not address the law regarding what is or is not considered privileged, other than to note that the Fifth Circuit has defined attorney-client privileged communications as (1) confidential communications (2) made to a lawyer or his subordinate (3) "for the primary purpose of securing either a legal opinion or legal services, or assistance in some legal proceeding." *United States v. Robinson*, 121 F.3d 971, 974 (5th Cir. 1997). The party asserting the work product doctrine—

must show that "the primary motivating purpose behind the creation of the document was to aid in possible future litigation," considering factors such

as the retention of counsel and his or her involvement in the generation of the document and whether it was routine to prepare such a document or it was instead prepared in response to a particular circumstance. "If the document would have been created without regard to whether litigation was expected to ensue, it was made in the ordinary course of business and not in anticipation of litigation."

Louis Vuitton Malletier v. Texas International Partnership, No. H-10-2821, 2012 WL 5954673, at *3 (S.D. Tex. May 14, 2012) (internal citations omitted).

§ 12.2 Texas Rule of Civil Procedure 193.3

Adopted in 1999, rule 193 of Texas Rules of Civil Procedure anticipated the difficulties ESI would pose when producing discovery. Rule 193.3(d) states the following:

Privilege not waived by production. A party who produces material or information without intending to waive a claim of privilege does not waive that claim under these rules or the Rules of Evidence if—within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made—the producing party amends the response, identifying the material or information produced and stating the privilege asserted. If the producing party thus amends the response to assert a privilege, the requesting party must promptly return the specified material or information and any copies pending any ruling by the court denying the privilege.

Tex. R. Civ. P. 193.3(d).

As stated by the Texas Supreme Court, this "snap-back provision" was "designed to protect the inadvertent disclosure of privileged material in order to reduce the cost and risk involved in document production." *See In re Christus Spohn Hospital Kleberg*, 222 S.W.3d 434, 438–39 (Tex. 2007) (orig. proceeding). The court further noted that—

the snap-back provision was designed to ensure that important privileges are not waived by mere inadvertence or mistake. Under the rule, a party who is less than diligent in screening documents before their production does not waive any privilege that might attach to them, presuming the party complies with rule 193.3(d)'s procedures. Tex. R. Civ. P. 193.3(d) cmt. 4. By permitting the recovery of documents inadvertently produced to the opposing side, the rule preserves the important interests that the workproduct doctrine was designed to protect, while at the same time visiting no harm upon the recipient for having to return documents it was not entitled to in the first place. Under rule 193.3(d), the production of documents without the intent to waive a claim of privilege does not waive the claim.

In re Christus Spohn, 222 S.W.3d at 39.1

Before September 2008, the federal rules did not provide for any relief from the inadvertent disclosure of privileged documents.

§ 12.3 Federal Cases Interpreting Waiver of Privilege before 2008

Before the United States Congress adopted Federal Rule of Evidence 502 in September 2008, the consequences of inadvertent disclosure varied by state: some jurisdictions held no waiver from inadvertent production; some jurisdictions took a strict liability approach, holding any production waived privilege; and many jurisdictions applied an intermediate balancing test to the facts of each case. *See Victor Stanley v. Creative Pipe, Inc.*, 250 F.R.D. 257–58; *Hopson v. Mayor & City Council of Baltimore*, 232 F.R.D. 228, 251, 235–36 (D. Md. 2008). The balancing test included factors such as the reasonableness of the precautions taken to prevent inadvertent disclosure in relation to the size of the production, the number of inadvertent disclosures, the time constraints on production, any delay and measures taken to rectify the disclosure, and the overriding interests of justice. *See, e.g., Fidelity & Deposit Co. of Maryland v. McCulloch*, 168 F.R.D. 516, 522 (E.D. Pa. 1996).

In addition, some courts took the position that failure to produce a privilege log or by providing an inadequate one deemed the privilege waived. *See In re Universal Serv. Fund Tel. Billing Practices Litig.*, 232 F.R.D. 669 (D. Kan. 2005) (listing e-mail strand as single document on privilege log is inadequate; rather, individual e-mails had to be separated from one another when evaluating privilege claim to avoid stealth claims of privilege).

§ 12.4 Federal Rule of Evidence 502

In light of the voluminous productions of ESI, especially in complex litigation, and the high attorney's fees associated with review prior to production to avoid the inad-

^{1.} See also In re City of Dickinson, 568 S.W.3d 642, 649 (Tex. 2019) (allowing for snap-back of attorney-client material produced).

vertent production of privileged documents, Congress adopted rule 502 in September 2008. Rule 502 seeks to create a uniform and predictable standard for inadvertent disclosure by limiting when a federal court will find waiver of privilege. See Fed. R. Evid. 502 advisory committee's note 2.

Rule 502 states in part—

- (a) Inadvertent Disclosure. When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if:
 - (1) the disclosure is inadvertent;
 - (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and
 - (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).
- (b) Disclosure Made in a State Proceeding. When the disclosure is made in a state proceeding and is not the subject of a state-court order concerning waiver, the disclosure does not operate as a waiver in a federal proceeding if the disclosure:
 - (1) would not be a waiver under this rule if it had been made in a federal proceeding; or
 - (2) is not a waiver under the law of the state where the disclosure occurred.
- (c) Controlling Effect of a Court Order. A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding.
- (d) Controlling Effect of a Party Agreement. An agreement on the effect of disclosure in a federal proceeding is binding only on the parties to the agreement, unless it is incorporated into a court order.
- (e) Controlling Effect of This Rule. Notwithstanding Rules 101 and 1101, this rule applies to state proceedings and to federal courtannexed and federal court-mandated arbitration proceedings, in the circumstances set out in the rule. And notwithstanding Rule 501, this rule applies even if state law provides the rule of decision.

- (f) Definitions. In this rule:
 - (1) "attorney-client privilege" means the protection that applicable law provides for confidential attorney-client communications; and
 - (2) "work-product protection" means the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial.

Fed. R. Evid. 502.

Rule 502(b) creates a three-part test that allows the producing party to avoid waiver when: "(1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B)." Fed. R. Evid. 502(b).

Rule 502 was intended to reduce the costs of preproduction privilege review by reducing the fear that even a minimal or inadvertent production of privileged documents would be deemed a waiver of privilege for all communications on similar subject matter. Fed. R. Evid. 502 advisory committee's notes 1–2. While this rule has prevented subject-matter waiver because of inadvertent production and has made the standards for finding waiver largely uniform, it still requires significant and costly preproduction review. *Bear Republic Brewing Co. v. Central City Brewing Co.*, 275 F.R.D. 43, 47–49 (D. Mass. 2011); *see First American CoreLogic, Inc. v. Fiserv, Inc.*, No. 2:10-CV-132-TJW, 2010 WL 4975566, at *5 (E.D. Tex. Dec. 2, 2010).

§ 12.4:1 Inadvertent Disclosure

Rule 502 begins by classifying production into two camps: intentional and inadvertent. The rule itself does not assign the burden of proving inadvertence, but courts consistently assign that burden to the party seeking claw-back of the privileged documents. *See, e.g., Amobi v. Dist. of Columbia Dep't of Corr.*, 262 F.R.D. 45, 53 (D.D.C. 2009); *Thorncreek Apartments III, LLC v. Village of Park Forest*, Nos. 08-C-1225, 08-C-0869, 08-C-4304, 2011 WL 3489828, at *6 (N.D. Ill. Aug. 9, 2011).

Although rule 502(b) does not define "inadvertent," most courts apply the first prong of the test permissively, asking only whether the disclosure was intended or mistaken. *See, e.g., Coburn Group, LLC v. Whitecap Advisors, LLC*, 640 F. Supp. 2d 1032, 1038 (N.D. Ill. 2009); *Kelly v. CSE Safeguard Insurance Co.*, No. 2:08-cv-88-KJD-RJJ,

2011 WL 3494235, at *2 (D. Nev. Aug. 10, 2011); *Amobi*, 262 F.R.D. at 53–54; *cf. First American CoreLogic, Inc. v. Fiserv, Inc.*, No. 2:10-CV-132-TJW, 2010 WL 4975566, at *4 (E.D. Tex. Dec. 2, 2010) (finding a disclosure intentional where counsel served privileged documents on other parties because the documents were filed under seal, rather than in camera and the documents did not indicate any intention to file in camera). Such a definition comports well with the structure and purpose of the rule and with the drafting committee's comments. *Coburn*, 640 F. Supp. 2d at 1038, n.4. Simplifying the threshold question allows a party asserting privilege to focus on the other two prongs of the test, for which parties can more easily marshal evidence.

§ 12.4:2 Reasonable Steps to Prevent Disclosure

After meeting the threshold of inadvertence, the producing party must show that it took "reasonable steps to prevent disclosure" of privileged documents. Fed. R. Evid. 502(b)(2). This second prong brings back the balancing test used in many jurisdictions before rule 502 was enacted. *See Eden Isle Marina, Inc. v. United States*, 89 Fed. Cl. 480, 502 (2009); *Coburn Group, LLC v. Whitecap Advisors, LLC*, 640 F. Supp. 2d 1032, 1038–39 (N.D. Ill. 2009). In deciding whether preproduction review was reasonable, courts will consider the methods used by the producing party in searching for and segregating privileged documents, including the extent of the disclosure relative to the entire production, the time constraints for production, and the experience of and supervision over the reviewers. *Coburn*, 640 F. Supp. 2d at 1038–39; *see Valentin v. Bank of New York Mellon Corp.*, No. 09 Civ. 9448(GBD)(JCF), 2011 WL 1466122, at *2–3 (S.D.N.Y. Apr. 14, 2011); *Comrie v. Ipsco, Inc.*, No. 08 C 3060, 2009 WL 4403364, at *2 (N.D. Ill. Nov. 30, 2009); *Clarke v. J.P. Morgan Chase & Co.*, No. 08 Civ. 02400(CM)(DF), 2009 WL 970940, at *5 (S.D.N.Y. Apr. 10, 2009).

The extent of the disclosure of privileged documents factors heavily into the analysis of whether a party took reasonable steps. Courts will often compare the percentage of inadvertently produced documents to the size of the overall production, though the percentage analysis "becomes less meaningful as the total number of documents diminishes." *Valentin*, 2011 WL 1466122, at *3; *see also Pacific Coast Steel v. Leany*, No. 2:09 cv-02190-KJD-PAL, 2011 WL 4704217, at *1–2 (D. Nov. Oct. 4, 2011); *Alers v. City of Philadelphia*, No. 08-4745, 2011 WL 6000602, at *2 (E.D. Pa. Nov. 29, 2011); *Diesel Machinery, Inc. v. Manitowoc Cranes, Inc.*, No. CIV 09-4087-RAL, 2011 WL 1343121, at *3 (D.S.D. Apr. 7, 2011).

If production is extensive or includes large volumes of ESI, even the inadvertent production of many privileged documents will not necessarily mean waiver of privilege.
"Inadvertent production of a relatively low proportion of documents in a large production under a short timetable due to mistake should be and usually is excused." *Datel Holdings Ltd. v. Microsoft Corp.*, No. C-09-05535 EDL, 2011 WL 866993, at *4 (N.D. Cal. Mar. 11, 2011); *see Valentin*, 2011 WL 1466122, at *2 (holding "the steps taken to preserve privilege need not be perfect; they must only be reasonable"). *Relion, Inc. v. Hydra Fuel Cell Corp.*, No. CV06-607-HU, 2008 WL 5122828, at *3 (D. Or. Dec. 4, 2008) (finding waiver where party did not use "all reasonable means" to preserve privilege). However, as the number and proportion of inadvertently produced documents increases, courts are less likely to find that counsel took reasonable precautions. *See Mt. Hawley Insurance Co. v. Felman Production, Inc.*, 271 F.R.D. 125, 128–130 (S.D. W. Va. 2010); *Thorncreek Apartments III, LLC v. Village of Park Forest*, Nos. 08-C-1225, 08-C-0869, 08-C-4304, 2011 WL 3489828, at *6–8 (N.D. Ill. Aug. 9, 2011) (finding waiver where counsel neither produced privilege log nor tested system of outside vendor, resulting in production of every privileged document).

Because the producing party has the burden of showing inadvertent disclosure, counsel must give the court details about the preproduction review in order to show reasonable precautions were taken. Courts expect specifics about how many pages were produced in total, how many privileged pages were produced, what keywords were used in ESI searches, who defined the keywords and the expertise of the searchdesigner, whether the keyword searches were tested before production, whether attorneys or paralegals completed the manual review after ESI searches, whether the review protocol was specific enough to alert the reviewers, whether a quality control review was completed, and whether the producing party completed a timely and thorough privilege log. *Datel*, 2011 WL 866993, at *4; *Mt. Hawley*, 271 F.R.D. at 134–36; *Coburn*, 640 F. Supp. 2d at 1038–1040; *Rhoads Indus., Inc. v. Bldg. Materials Corp. of America*, 254 F.R.D. 216, 226–27 (E.D. Pa. 2008); Victor Stanley, 250 F.R.D. at 261–63; *see Williams v. Dist. of Columbia*, 806 F. Supp. 2d 44, 50–51 (D.D.C. 2011); *Thorncreek Apartments*, 2011 WL 3489828, at *6; *Eden Isle*, 89 Fed. Cl. at 497–02, 506–15.

If a party does not give sufficient specific evidence about the review or does not produce an adequate or timely privilege log, courts often find they have not met their burden to show reasonable precautions to prevent disclosure. *Williams*, 806 F. Supp. 2d at 49–51; *Sidney I. v. Focused Retail Property I, LLC*, 274 F.R.D. 212, 216–17 (N.D. III. 2011); *Amobi v. Dist. of Columbia Dept. of Corr.*, 262 F.R.D. 45, 53–54 (D.D.C. 2009). Courts may consider facts other than the preproduction review in deciding whether counsel took measures adequate to protect privileged documents. For instance, if a privileged document is produced more than once, especially if by more than one mechanism, a court is likely to find the disclosure so careless as to waive the privilege. *Eden Isle*, 89 Fed. Cl. at 515 (2009). Or, following notice of an inadvertent production, the court may expect the producing party to reassess its review procedure and search for other documents that may have been inadvertently produced. *See, e.g., Luna Gaming-San Diego, LLC v. Dorsey & Whitney, LLP*, No. 06cv2804 BTM (WMc), 2010 WL 275083, at *6–7 (S.D. Cal. Jan. 13, 2010). Failure to conduct a postproduction review, absent notice of an inadvertent disclosure, will not cause a court to find waiver. *Coburn*, 640 F. Supp. 2d at 1040.

§ 12.4:3 Reasonable Steps to Rectify the Error

In addition to preproduction review, rule 502(b) requires the privilege-holder to promptly take "reasonable steps to rectify the error" in production. Fed. R. Evid. 502(b); see, e.g., Eden Isle Marina, Inc. v. United States, 89 Fed. Cl., 510-11. Rather than judging from the time of production, the relevant time period is "how long it took the producing party to act after it learned that the privileged or protected document had been produced." Coburn Group, LLC v. Whitecap Advisors, LLC, 640 F. Supp. 2d 1032, 1041 (N.D. Ill. 2009). Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251, 263 (D. Md. 2005) (finding waiver in part because producing party did not discover after inadvertent production until notified by opposition). Since attorneys commonly discover inadvertent disclosures at depositions, counsel should object to the use of the document at the deposition and prevent further questioning on that document. See Pacific Coast Steel v. Leanv, No. 2:09-cv-02190-KJD-PAL, 2011 WL 4704217, at *1 (D. Nev. Oct. 4, 2011); Datel Holdings Ltd. v. Microsoft Corp., No. C-09-05535 EDL, 2011 WL 866993, at *5 (N.D. Cal. Mar. 11, 2011); Sidney I. v. Focused Retail Prop. I, LLC, 274 F.R.D. 212, 217-218 (N.D. III. 2011); AHF Comm. Dev., LLC v. City of Dallas, 258 F.R.D. 143 (N.D. Tex. 2009) (privilege waived when documents marked attorney-client privilege were used at deposition); Coburn, 640 F. Supp. 2d at 1041. Cf. Alers v. City of Philadelphia, No. 08-475, 2011 WL 6000602, at *2-3 (E.D. Pa. Nov. 29, 2011) (finding no waiver despite lack of objection at deposition and four-day delay before requesting return of document because nonproducing party did not honor ethical obligation to return obviously privileged document). A demand letter, even one sent the next day, may not prevent waiver if a privileged document is used at a deposition without objection and the deponent answers questions about the document. Sidney I., 274 F.R.D. at 218.

Privilege Waiver, Rule 502, and Clawback/Sneak Peek Agreements

While rule 502(b)(3) requires prompt action to prevent waiver, the length of the permissible delay varies according to the facts of the case. If counsel objects at the depcsition and then takes some time to investigate the facts of the disclosure, or if both sides confer in an attempt to solve the problem informally, courts will accept a few weeks between notice and filing a motion. *Pacific Coast Steel*, 2011 WL 4704217, at *6; *Williams v. Dist. of Columbia*, 806 F. Supp. 2d 44, 52 (D.D.C. 2011) (stating that producing party should attempt to meet and confer in order to resolve inadvertent disclosure disputes without the court); *Coburn*, 640 F. Supp. 2d at 1041 (holding that three weeks of investigation before filing motion was not waiver).

If the inadvertent disclosure is not discovered at a deposition or where circumstances do not permit such an immediate objection on the record, one court considered as prompt a six-day delay between discovery of the inadvertent production and demancing the return of the document. *Valentin v. Bank of New York, Mellon Corp.*, No. 09 Civ. 9448(GBD)(JCF), 2011 WL 1465122, at *3 (S.D.N.Y. Apr. 14, 2011). A safer course of action, however, would be to demand the return or destruction of the document the day of or day after discovering the inadvertent disclosure.

If, however, a party fails to quickly demand return or fails to follow up on its initial demand for return of a document, courts are far more likely to find waiver. *Williams*, 806 F. Supp. 2d at 52 (finding waiver where producing party did not follow up on its initial demand for two years and nine months); *Clarke v. J.P. Morgan Chase & Co.*, No. 08 Civ. 02400(CM)(DF), 2009 WL 970940, at *6 (S.D.N.Y. Apr. 10, 2009) (fincing waiver where privilege was asserted two months after discovering production); *Rhoads Indus., Inc. v. Bldg. Materials Corp. of America*, 254 F.R.D. 216, 225 (E.D. Pa. 2008) (finding waiver where producing party did not produce privilege log for inadvertently disclosed documents until four months after notice). Thus, a party that inadvertently produces privileged documents will most likely prevent waiver under rule 502(b) if counsel acts quickly.

§ 12.5 Federal Rule of Civil Procedure 26(b)(5)(B)

As soon as a party becomes aware that it has inadvertently disclosed privileged documents, the party should immediately comply with Fed. R. Civ. P. 26(b)(5)(B). This rule states the following:

Information Produced. If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the

claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.

Fed. R. Civ. P. 26(b)(5)(B).²

§ 12.6 Order Pursuant to Federal Rule of Evidence 502(d)

In light of the conflicting case law concerning what were reasonable steps to prevent disclosure and what were reasonable steps to rectify the error, it is highly advisable that the parties obtain an order in their federal court proceeding that privilege or protection is not waived by disclosure connected with the litigation pending before the court. *See* Fed. R. Evid. 502(d). This order should be discussed by the parties at the "meet and confer" conference,³ can be obtained very early in this case, generally at the Fed. R. Civ. P. 16 initial conference,⁴ and prior to the exchange of discovery. Sample language of such an order that incorporates rule 502(d), written by former U.S. Magistrate Judge Andrew Peck, follows:

 The production of privileged or work-product protected documents, electronically stored information (ESI) or information, whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d).

^{2.} Privilege is waived for inadvertently produced documents when the producing party fails to establish the reasonableness of the precautions taken to prevent disclosure and fails "to take adequate measures to rectify or mitigate the damage of the disclosure." *Inhalation Plastics, Inc. v. Medex Cardio-Pulmonary, Inc.*, No. 2:07-CV-116, 2012 WL 3731483, at *5 (S.D. Ohio Aug. 28, 2012). (Defendant was found to have waived the attorney-client privilege as to 347 pages of inadvertently produced e-mails. Defendant did not take reasonable precautions to prevent the disclosure. In addition, Defendant failed to follow the procedure in Fed. R. Civ. P. 26(b)(5)(B), never providing a privilege log and, beyond conclusory statements, not stating a basis for the claimed privilege.)

^{3.} Fed. R. Civ. P. 26(f)(3)(D) (any issues about claims of privilege or of protection as trial-preparation materials, including—if the parties agree on a procedure to assert these claims after production—whether to ask the court to include their agreement in an order).

^{4.} Fed. R. Civ. P. 16(b)(3)(B)(iv) (include any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after information is produced).

 Nothing contained herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI or information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production.⁵

Many commentators have referred to 502(d) as a "get out of jail card" inasmuch as a party that inadvertently produces attorney-client privilege of work-product material may avoid waiver, without having to establish all the elements set forth in 502(b). Despite its intent to reduce the costs of litigation, anecdotal evidence suggests the provision for a court order is seldom requested by any party.⁶

§ 12.7 Federal Rule of Evidence 502(e) and Clawback and Sneak Peek Agreements

Nonwaiver of privilege agreements have two general descriptions: (1) a "clawback" agreement and (2) a "sneak peek" or "quick peek" agreement. A clawback agreement allows the producing party to "claw back" the privileged document once discovered. A "sneak peek" allows the requesting party to review ESI and designate what information it wants produced pursuant to a Fed. R. Civ. P. 34 request. Then the producing party reviews the designated information for privilege.

If the parties decide to enter into a clawback or sneak peek agreement, it is highly advisable that they include such an agreement in the court's rule 502(d) protective order. Failure to memorialize the agreement in an order can order can result in the court finding the agreement is not binding.⁷

Rule 502(e) explicitly codifies the availability of such agreements. Parties entering such agreements should include language about what constitutes reasonable precau-

^{5.} The addition of this second paragraph is becoming more common in rule 502(d) orders. The provision is important to prevent a court from ordering a "quick peek" for the requesting party. *See Fairholme Funds, Inc. v. United States*, 134 Fed. Cl 680 (2017) (even without the producing party's consent, the court entered a Fed. R. Evid. 502(d) quick peek order allowing the requesting party to review documents being withheld as privileged). *But see Winfield v. City of New York*, No. 15-cv-05236 (LTS) (KHP), 2018 WL 2148435 (S.D.N.Y. May 10, 2018) (a court may not compel a "quick peek" of privileged documents over a party's objection).

^{6.} See *Bellamy v. Wal-Mart Stores, Texas, LLC*, No. SA-18-CV-60-XR, 2019 WL 3936992, at *1 (W.D. Tex. Aug. 19, 2019) (court encouraged parties to enter a 502(d) Order, they declined, and Defendant thereafter produced privileged documents necessitating a 502(b) analysis).

^{7.} See Irth Sols. v. Windstream Commc'ns LLC, No. 2:16-cv-219, 2017 WL 3276021 (S.D. Ohio Aug. 2, 2017) (where the operative clawback agreement, which was not reduced to an order, is so perfunctory that its intentions are not clear, producing party may waive the attorney-client privilege where it recklessly produces privileged documents).

§ 12.7

tions, including use of a software review system as being a reasonable precaution. Rule 502(d) should be referenced in the clawback agreement.⁸ If the parties cannot agree, a court may add clawback provisions to protective orders in cases (especially with large ESI productions), even over the objections of a party. *Rajala v. McGuire Woods, LLP*, No. 08-2638-CM-DJW, 2010 WL 2949582, at *6–7 (D. Kan. July 22, 2010).

§ 12.8 Conclusion

Given the sheer volume of discovery production, it is quite probable that even with best efforts exerted, there will be an inadvertent disclosure of privileged documents. A producing party in a case pending before a Texas state court has the ability to invoke Tex. R. Civ. P. 193.3, assuming that within ten days (or a shorter time ordered by the court) after the producing party actually discovers that such production was made, it amends its discovery response, identifies the material or information inadvertently produced, and states the privilege asserted. Litigants in the Texas state courts must remain wary, however, because the other benefits of Fed. R. Evid. 502(d) and (e) are not available in the Texas courts.

Litigants in the federal courts should take full advantage of Fed. R. Evid. 502(d) and (e).⁹ Anecdotal evidence suggests that rule 502 is utilized infrequently. Many commentators and federal judges are baffled by litigants' failure to utilize this rule. Rule 502(d) orders should expressly state that rule 502(b) does not apply.

Finally, whether the litigation is in the state or federal court system, if the litigation is complex enough, if it implicates a large discovery ESI review and production, and if the financial stakes are great, the parties should consider the retention of discovery special masters. *See* Tex. R. Civ. P. 171; Fed. R. Civ. P. 53. Such a special master or "e-neutral" can assist in the drafting of any clawback or sneak peek agreements, tailor appropriate privilege log protocols, and otherwise assist in minimizing the expense associated with discovery review and production. See Chapter 17—Mediation of E-Discovery Disputes and Special Masters for additional guidance on this topic.

^{8.} See also Noam Noked, Best Practices for Preparing a Clawback Agreement, The Harvard Law School Forum on Corporate Governance and Financial Regulation (Nov. 21, 2012), http://blogs.law.harvard.edu/corpgov/2012/11/21/best-practices-for-preparing-a-clawback-agreement/.

^{9.} See Thomas C. Gricks, III, The Effective Use of Rule 502(d) in E-Discovery Cases, The Legal Intelligencer (Oct. 25, 2011), www.schnader.com/files/Publication/3e1f43b1-dd2f-4dcf-9c33 -2ff841b72993/Presentation/PublicationAttachment/092279b5-c685-46bf-8db3-3360f54a5dc2/ Gricks_Legal%20Article_Oct.%202011.pdf.

Chapter 13

Responding to Discovery Requests and Discovery Disputes

Judge David L. Horan

§ 13.1 Introduction

Parties may discover electronically stored information ("ESI") from other parties and third parties under the Federal Rules of Civil Procedure and the Texas Rules of Civil Procedure. These sets of rules govern what a party must do to properly request ESI, how parties or third parties must respond to discovery requests for ESI, and how to resolve disputes about whether, when, and how ESI should be discovered.

§ 13.2 Federal Court

The Federal Rules of Civil Procedure control the scope of a proper discovery request for ESI as well as how to properly respond to such a request. Amendments effective December 1, 2015 significantly changed certain rules and their operation.

§ 13.2:1 Federal Rules of Civil Procedure 26(b)(1), 26(b)(2), and 26(g)

Under Federal Rule of Civil Procedure 26(b)(1),

[u]nless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.¹

"Information within this scope of discovery need not be admissible in evidence to be discoverable."²

^{1.} Fed. R. Civ. P. 26(b)(1).

The 2015 amendments to rule 26 deleted "from the definition of relevance information that appears 'reasonably calculated to lead to the discovery of admissible evidence' because '[t]he phrase has been used by some, incorrectly, to define the scope of discovery' and 'has continued to create problems' given its ability to 'swallow any other limitation on the scope of discovery."³

After the 2015 amendments to Federal Rule of Civil Procedure 26, an objection that discovery requests are not "reasonably calculated to lead to the discovery of admissible evidence" is no longer proper.⁴

"Under Rule 26(b)(1), [as amended,] discoverable matter must be both relevant and proportional to the needs of the case—which are related but distinct requirements."⁵

"To be relevant under rule 26(b)(1), a document or information need not, by itself, prove or disprove a claim or defense or have strong probative force or value"⁶ "If it were otherwise, it would make little sense for rule 26(b)(1) to direct courts to consider whether discovery that is relevant to any party's claim or defense is also important in resolving the issues."⁷

As amended, Federal Rule of Civil Procedure 26(b)(2)(C) provides-

On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or (iii) the proposed discovery is outside the scope permitted by rule 26(b)(1).⁸

4. *Crum & Forster Specialty Ins. Co. v. Great West Casualty Co.*, No. EP-15-cv-00325-DCG, 2016 WL 10459397, at *4 n.5 (W.D. Tex. Dec. 28, 2016).

5. Samsung Electronics Am., Inc. v. Chung, 321 F.R.D. 250, 279 (N.D. Tex. 2017).

6. Samsung Electronics, 321 F.R.D. at 280; see also Deutsche Bank National Trust Company v. Pink, No. 7:18-cv-20-O-BP, 2019 WL 399533, at *5 (N.D. Tex. Jan. 31, 2019).

7. Samsung Electronics, 321 F.R.D. at 280.

8. Fed. R. Civ. P. 26(b)(2)(C).

^{2.} Fed. R. Civ. P. 26(b)(1).

^{3.} State Auto. Mut. Ins. Co. v. Freehold Mgmt., Inc., No. 3:16-cv-2255-L, 2018 WL 3548866, at *2 (N.D. Tex. July 24, 2018) (quoting *Robroy Indus.-Tex., LLC v. Thomas & Betts Corp.*, No. 2:15-CV-512-WCB, 2017 WL 319064, at *4 (E.D. Tex. Jan. 23, 2017) (quoting Fed. R. Civ. P. 26, 2015 committee note)).

Federal Rule of Civil Procedure 26(b)(2)(B) also provides specific limitations on ESI:

A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of rule 26(b)(2)(C). The court may specify conditions for the discovery.⁹

"Rule 26(b)(2)(B) allows the party resisting production of [ESI] to avoid production if such ESI is not reasonably accessible because of undue burden or cost. The rule 26(b)(2)(B) analysis considers factors such as the complexity of the ESI and the nature of the media on which the ESI is stored."¹⁰ And courts have held that "[a] party resisting the production of relevant electronically stored information must submit evidentiary proof 'that the information is not reasonably accessible because of undue burden or cost."¹¹ Rule 26(b)(2)(B)'s provisions are otherwise discussed more fully elsewhere in this chapter.

And, as to any discovery, whether seeking ESI or otherwise, the Federal Rules of Civil Procedure require that attorneys or unrepresented parties comply with the rules' limits on the scope of discovery requests. Federal Rule of Civil Procedure 26(g) provides:

Signing Disclosures and Discovery Requests, Responses, and Objections.

(1) Signature Required; Effect of Signature. Every disclosure under rule 26(a)(1) or (a)(3) and every discovery request, response, or objection must be signed by at least one attorney of record in the attorney's own name—or by the party personally, if unrepresented—and must

11. American Airlines, Inc. v. Travelport Limited, No. 4:11-CV-244-Y, 2012 WL 12884821, at *2 (N.D. Tex. May 29, 2012) (quoting Fed. R. Civ. P. 26(b)(2)(B); citing Auto Club Family Ins. Co. v. Ahner, No. 05-05723, 2007 WL 2480322, at *3 (E.D. La. Aug. 29, 2007)).

^{9.} Fed. R. Civ. P. 26(b)(2)(B).

^{10.} Hall v. Rent-A-Center, Inc., Civ. A. No. 4:16cv978, 2018 WL 4293141, at *2 (E.D. Tex. Aug. 31, 2018) (citing KAIST IP US LLC v. Samsung Elecs. Co., Ltd., No. 2:16-CV-01314-JRG-RSP, 2017 WL 9937760, at *2 (E.D. Tex. Dec. 21, 2017) (citing Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 318–19 (S.D.N.Y. 2003) ("[W]hether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format (a distinction that corresponds closely to the expense of production)."))).

state the signer's address, e-mail address, and telephone number. By signing, an attorney or party certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry:

- (A) with respect to a disclosure, it is complete and correct as of the time it is made; and
- (B) with respect to a discovery request, response, or objection, it is:
 - (i) consistent with these rules and warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law, or for establishing new law;
 - (ii) not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and
 - (iii) neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action.

....

(3) Sanction for Improper Certification. If a certification violates this rule without substantial justification, the court, on motion or on its own, must impose an appropriate sanction on the signer, the party on whose behalf the signer was acting, or both. The sanction may include an order to pay the reasonable expenses, including attorney's fees, caused by the violation.¹²

"Rule 26(g) imposes an affirmative duty to engage in pretrial discovery in a responsible manner that is consistent with the spirit and purposes of rules 26 through 37."¹³

Rule 26(g) specifically "requires that parties make a reasonable inquiry before conducting or opposing discovery."¹⁴ This "provides a deterrent to both excessive discovery and evasion by imposing a certification requirement that obliges each attorney to

^{12.} Fed. R. Civ. P. 26(g)(1) and (g)(3).

^{13.} Fed. R. Civ. P. 26, 1983 committee note.

^{14.} Smith v. Our Lady of the Lake Hosp., Inc., 960 F.2d 439, 448 (5th Cir. 1992).

stop and think about the legitimacy of a discovery request, a response thereto, or an objection" and whether it is consistent with the Federal Rules of Civil Procedure and "grounded on a theory that is reasonable under the precedents or a good faith belief as to what should be the law."¹⁵

Although the certification duty requires the lawyer to pause and consider the reasonableness of his request, response, or objection, it is not meant to discourage or restrict necessary and legitimate discovery. The rule simply requires that the attorney make a reasonable inquiry into the factual basis of his response, request, or objection.¹⁶

The duty to make a 'reasonable inquiry' is satisfied if the investigation undertaken by the attorney and the conclusions drawn therefrom are reasonable under the circumstances. It is an objective standard similar to the one imposed by [Federal Rule of Civil Procedure] 11.... Ultimately what is reasonable is a matter for the court to decide on the totality of the circumstances.¹⁷

"Rule 26(g) was enacted 'to eliminate one of the most prevalent of all discovery abuses: kneejerk discovery requests served without consideration of cost or burden to the responding party."¹⁸ By signing discovery requests, the attorney or party serving discovery requests makes an affirmative certification that the requests are not unreasonable or unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action.¹⁹

If the requests nevertheless fall outside the rule 26(b)(1) scope of discovery, the serving attorney or party may face Federal Rule of Civil Procedure 26(g)(3) sanctions if the attorney or party made the certification without substantial justification.²⁰

17. *Chapman & Cole v. Itel Container Int'l B.V.*, 865 F.2d 676, 686 (5th Cir. 1989) (quoting Fed. R. Civ. P. 26, 1983 committee note).

19. See Fed. R. Civ. P. 26(b)(1), 26(g)(1); accord Schlafly v. Caro-Kann Corp., 155 F.3d 565, 1998 WL 205766, at *3 (Fed. Cir. Apr. 28, 1998) (explaining that a party requesting discovery under rule 34 "has the burden to state his discovery requests with reasonable particularity and not to make unreasonably cumulative or duplicative requests such that the burden or expense of complying with the requests outweighs their likely benefit").

20. See Fed. R. Civ. P. 26(g)(1)(B), 26(g)(3); Heller, 303 F.R.D. at 475-77.

^{15.} Fed. R. Civ. P. 26, 1983 committee note.

^{16.} Fed. R. Civ. P. 26, 1983 committee note.

^{18.} Heller v. City of Dallas, 303 F.R.D. 466, 477 (N.D. Tex. 2014); (quoting Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354, 358 (D. Md 2008)).

The United States Supreme Court has defined "substantially justified" to mean justified in substance or in the main—that is, justified to a degree that could satisfy a reasonable person. "Substantial justification" entails a reasonable basis in both law and fact, such that there is a genuine dispute ... or if reasonable people could differ [as to the appropriateness of the contested action].²¹

The United States Court of Appeals for the Fifth Circuit has explained that "[s]ubstantial justification for the failure to make a required disclosure has been regarded as justification to a degree that could satisfy a reasonable person that parties could differ as to whether the party was required to comply with the disclosure [obligation]" and that "[t]he attorney's decision to refrain from disclosing the information must have had a reasonable basis both in law and fact."²²

§ 13.2:2 Federal Rule of Civil Procedure 34

Requirements for Request: As to requests for production, Federal Rule of Civil Procedure 34(a)(1) provides—

A party may serve on any other party a request within the scope of rule 26(b): (1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control: (A) any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilation—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form; or (B) any designated tangible things.²³

Properly responding or objecting to a rule 34(a) request requires an attorney to understand and consider rule 34's limitations on a request's scope and form.

Federal Rule of Civil Procedure 34(b) provides that a request for production or inspection "must describe with reasonable particularity each item or category of items to be inspected" or produced.²⁴ "The test for reasonable particularity is whether the

^{21.} Heller v. City of Dallas, 303 F.R.D. 466, 475-77 (N.D. Tex. 2014) (citations and emphasis omitted)).

^{22.} Olivarez v. GEO Group, Inc., 844 F.3d 200, 205 (5th Cir. 2016) (internal quotation marks and citations omitted).

^{23.} Fed. R. Civ. P. 34(a).

request places the party upon 'reasonable notice of what is called for and what is not."²⁵ "[T]he party requesting the production of documents must provide 'sufficient information to enable [the party to whom the request is directed] to identify responsive documents."²⁶ "The goal is that the description be sufficient to apprise a man of ordinary intelligence which documents are required."²⁷

"This test, however, is a matter of degree depending on the circumstances of the case."²⁸ But, although—

what qualifies as "reasonabl[y] particular" surely depends at least in part on the circumstances of each case, a discovery request should be sufficiently definite and limited in scope that it can be said to apprise a person of ordinary intelligence what documents are required and [to enable] the court . . . to ascertain whether the requested documents have been produced.²⁹

A rule 34(a) request made with reasonable particularity is one that does not require a reasonable attorney or party attempting to properly respond "to ponder and to speculate in order to decide what is and what is not responsive."³⁰ "'All-encompassing demands' that do not allow a reasonable person to ascertain which documents are required do not meet the particularity standard of rule 34(b)(1)(A)."³¹

For example, "[b]road and undirected requests for all documents which relate in any way to the complaint" do not meet rule 34(b)(1)(A)'s standard.³² Similarly, "[a] request for 'all documents and records' that relate to 'any of the issues,' while convenient, fails to set forth with reasonable particularity the items or category of items

26. Hager, 267 F.R.D. at 493 (quoting Kidwiler v. Progressive Paloverde Ins. Co., 192 F.R.D. at 202.

27. Vailes v. Rapides Par. Sch. Bd., No. CV 15-429, 2016 WL 744559, at *4 (W.D. La. Feb. 22, 2016) (quoting United States v. Nat'l Steel Corp., 26 F.R.D. 607, 610 (S.D. Tex. 1960)).

28. Hager, 267 F.R.D. at 493.

29. Regan-Touhy v. Walgreen Co., 526 F.3d 641, 649-50 (10th Cir. 2008).

30. Bruggeman ex rel. Bruggeman v. Blagojevich, 219 F.R.D. 430, 436 (N.D. III. 2004) (citing Pulsecard, Inc. v. Discover Card Servs., Inc., No. CIV.A.94-2304-EEO, 1995 WL 526533, at *3 (D. Kan. Aug. 31, 1995)).

31. In re Asbestos Prods. Liab. Litig. (No. VI), 256 F.R.D. 151, 157 (E.D. Pa. 2009).

32. Parsons v. Jefferson-Pilot Corp., 141 F.R.D. 408, 412 (M.D.N.C. 1992).

^{24.} Fed. R. Civ. P. 34(b)(1)(A).

^{25.} Hager v. Graham, 267 F.R.D. 486, 493 (N.D. W. Va. 2010) (quoting Kidwiler v. Progressive Paloverde Ins. Co., 192 F.R.D. 193, 202 (N.D. W. Va. 2000)).

sought for [the responding party's] identification and production of responsive documents."³³ Based on these rules, Texas federal courts have, for example—

- sustained objections to rule 34(a) requests for "[a]ll documents which evidence, describe, concern, or otherwise relate to the allegations in your Complaint" and "[a]ll documents not previously produced that support, contradict, or otherwise relate in any way to any of the allegations you have made in this lawsuit";³⁴ and
- sustained an objection to a rule 34(a) request for "[a]ll e-mail, electronically stored information, audiotapes, telephone messages, press releases, interviews, notes, documents, and other communications by and involving Chief David Brown and all subordinates where such communications relates [sic] in any way to [the plaintiff], her family, and any of the facts alleged in the Plaintiffs' Complaint."³⁵

It is no answer for attorneys serving blockbuster or all-encompassing or broad and undirected requests for production to say that they are not certain what the responding party has in its possession, custody, or control and do not want to miss anything—and so will ask for, effectively, everything.

Requests must be made in compliance with the federal rules discussed above and, if further discovery or investigation later reveals the existence or possible existence of additional relevant materials or information within rule 26(b)(1)'s scope, counsel can serve additional discovery requests and, if necessary, seek leave to do so.

Requirements for Responses: In response to a rule 34(a) request, "[f]or each item or category, the response must either state that inspection and related activities will be permitted as requested or state with specificity the grounds for objecting to the request, including the reasons."³⁶ "The responding party may state that it will produce copies of documents or of electronically stored information instead of permitting

^{33.} Sewell v. D'Alessandro & Woodyard, Inc., No. 2:07-CV-343-FTM-29, 2011 WL 843962, at *2 (M.D. Fla. Mar. 8, 2011); see also S.E.C. v. Mazzo, No. SACV121327DOCAN, 2013 WL 12172628, at *20 (C.D. Cal. Oct. 24, 2013) ("Boilerplate requests, like boilerplate objections, are not recognized and constitute an abuse of the discovery process.").

^{34.} *Gondola v. USMD PPM, LLC*, 223 F. Supp. 3d 575, No. 3:15-cv-411-M, 2016 WL 3031852, at *9 (N.D. Tex. May 27, 2016).

^{35.} Cook v. City of Dallas, No. 3:12-cv-3788-N, 2017 WL 9534098, at *9 (N.D. Tex. Apr. 10, 2017).

^{36.} Fed. R. Civ. P. 34(b)(2)(B).

Responding to Discovery Requests and Discovery Disputes

inspection. The production must then be completed no later than the time for inspection specified in the request or another reasonable time specified in the response."³⁷

And, "[i]n responding to [rule 34] discovery requests, a reasonable inquiry must be made, and if no responsive documents or tangible things exist, Fed. R. Civ. P. 26(g)(1), the responding party should so state with sufficient specificity to allow the Court to determine whether the party made a reasonable inquiry and exercised due diligence."³⁸

"If responsive documents do exist but the responsive party claims lack of possession, control, or custody, the party must so state with sufficient specificity to allow the Court (1) to conclude that the responses were made after a case-specific evaluation and (2) to evaluate the merit of that response."³⁹

Federal Rule of Civil Procedure 34(b)(2)(E) further provides that—

[u]nless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information [("ESI")]: (i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request; (ii) If α request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and (iii) A party need not produce the same electronically stored information in more than one form.⁴⁰

This requirement for production is discussed more fully elsewhere in this chapter.

39. Heller, 303 F.R.D. at 485 (internal quotation marks and citations omitted).

40. Fed. R. Civ. P. 34(b)(2)(E); see also McKinney/Pearl Rest. Partners, L.P. v. Metro. Life Ins. Co., 322 F.R.D. 235, 249 (N.D. Tex. 2016) (concluding "that, where rule 34(b)(2)(E)(i) addresses the organization of a production and rule 34(b)(2)(E)(i) specifically addresses the form for producing ESI (where form of production is inherently not an issue with hard-copy documents), and in light of the purposes of the 2006 amendments to rule 34 and of rule 34(b)(2)(E)(i)'s requirements, rules 34(b)(2)(E)(i) and 34(b)(2)(E)(i) should both apply to ESI productions."); *Turner v. Nationstar Mortg. LLC*, No. 3:14-cv-1704-L-BN, 2015 WL 11120879, at *2 (N.D. Tex. May 14, 2015) (explaining that to comply with rule 34(b)(2)(E)(i), "Rule 34 requires a party to [either] produce documents as they are kept in the usual course of business or to organize and label them tc correspond to the categories in the request—the party is not required to do both").

^{37.} Fed. R. Civ. P. 34(b)(2)(B).

^{38.} Heller, 303 F.R.D. at 485 (internal quotation marks and citations omitted).

And a party cannot refuse to engage in—and is not excused from being subjected to discovery because the discovery is relevant to a claim on which the resisting party believes that it will or should prevail.⁴¹

"Neither may a party refuse to comply with an opposing party's discovery requests simply because he believes that the opposing parties ha[ve] not fully complied with his discovery requests to them."⁴²

Requirements for Objections: In response to a rule 34(a) request, "[a]n objection must state whether any responsive materials are being withheld on the basis of that objection. An objection to part of a request must specify the part and permit inspection of the rest."⁴³

General or boilerplate objections are invalid, and "[o]bjections to discovery must be made with specificity, and the responding party has the obligation to explain and support its objections." Amended Federal Rule of Civil Procedure 34(b)(2)[(C)] effectively codifies this requirement, at least in part."⁴⁴ As one judge explained by way of example:

Nearly all of Defendant's responses begin with the objection:

Objection. Defendant would object to this request as it is overbroad, unduly burdensome, and harassing. Defendant would further object as the information requested is neither relevant nor reasonably calculated to lead

44. Orchestratehr, Inc. v. Trombetta, 178 F. Supp. 3d 476, 507 (N.D. Tex. 2016) (citing Heller, 303 F.R.D. at 483), objections overruled, No. 3:13-cv-2110-KS, 2016 WL 5942223 (N.D. Tex. Oct. 13, 2016); see also Kilmon v. Saulsbury Industries, Inc., No. MO:17-CV-99, 2018 WL 5800757, at *3 (W.D. Tex. Feb. 28, 2018).

^{41.} See Heller, 303 F.R.D. at 489 (citing *Third Pentacle, LLC v. Interactive Life Forms, LLC*, No. 3:10cv00238, 2012 WL 27473, at *3 (S.D. Ohio Jan. 5, 2012) (even if a party "presently holds a strong belief in the merits of [the party's] litigation positions, [the party's] strong belief—whether ultimately justified or not—provides no basis for avoiding [the party's] discovery obligations created by the Federal Rules of Civil Procedure")).

^{42.} Lopez v. Don Herring Ltd., 327 F.R.D. 567, 581 (N.D. Tex. 2018) (internal quotation marks omitted; citing Genentech, Inc. v. Trustees of Univ. of Pa., No. C 10-02037, 2011 WL 7074208, at *1 (N.D. Cal. June 10, 2011) ("The Court does not look favorably upon a 'tit-for-tat' approach to discovery. A party may not withhold relevant discovery simply on the basis that the other side has not been forth-coming with discovery. A party may not excuse its failure to comply with discovery obligations by claiming that its opposing party is similarly delinquent. Nor may a party condition its compliance with its discovery obligations on receiving discovery from its opponent.") (internal quotations and citations omitted); cf. Fed. R. Civ. P. 26(d)(2) ("Sequence. Unless, on motion, the court orders otherwise for the parties' and witnesses' convenience and in the interests of justice: (A) methods of discovery may be used in any sequence; and (B) discovery by one party does not require any other party to delay its discovery.").

^{43.} Fed. R. Civ. P. 34(b)(2)(C).

to the discovery of admissible evidence. Defendant would further object in that, on the advice of counsel, Defendant asserts his right against selfincrimination as afforded by the Fifth Amendment to the United States Constitution and pursuant to Article 1, Section 10 of the Texas Constitution.

[Defendant] argues that his objections, including the one above, are not boilerplate because "[e]ach of those objections is appropriate and applicable to the specific items sought in Plaintiff's Request for Production." (Dkt. #26 at p. 7). The Court disagrees.

"Boilerplate" means "standardized text" or "ready-made or all-purpose language." Boilerplate, Merriam-Webster Collegiate Dictionary (11th ed. 2007); Boilerplate, Black's Law Dictionary (10th ed. 2014). Defendant used the above objections on all nine (9) of his RFP responses. This is the epitome of "standardized text." Simply put, the above over broad, unduly burdensome, relevance objections do not "state with specificity the grounds for objecting to the request." Fed. R. Civ. P. 34(b)(2)(B).⁴⁵

In sum, "[a] party served with written discovery must fully answer each interrogatory or document request to the full extent that it is not objectionable and affirmatively explain what portion of an interrogatory or document request is objectionable and why, affirmatively explain what portion of the interrogatory or document request is not objectionable and the subject of the answer or response, and affirmatively explain whether any responsive information or documents have been withheld."⁴⁶

As one judge has explained an example of how not to do this right:

Much of the confusion comes from Wal-Mart's overabundance of caution in responding under the new discovery rules, which now require that when a party makes an objection, it also state whether it is withholding any documents subject to that objection. In every one of its responses to TPSA's requests, Wal-Mart has leveled one or more objection, and in each instance it states that it is withholding documents pursuant to that objection. TPSA was therefore concerned that there are identified, responsive documents sitting on Wal-Mart's counsel's desk that have not been produced, any of which may be a "bombshell."

^{45.} Tsanacas v. Amazon.com, Inc., No. 4:17-CV-306, 2018 WL 324447, at *3 (E.D. Tex. Jan. 8, 2018) (citations omitted).

^{46.} Heller, 303 F.R.D. at 485.

According to the above discussion, the objection that Wal-Mart was withholding documents . . . was the result of Wal-Mart's understanding that it was required to make that statement even if it had not actually identified any responsive documents. While such a statement is perhaps literally compliant with the new rule, it is likely not truly what the rule is aiming for.

This is best understood with an example. In RFP 16, TPSA requests Wal-Mart to produce documents "relating to any allegation that [Wal-Mart] ha[s] engaged in predatory pricing." Dkt. No. 179-1 at 9. Wal-Mart's response to this request states:

Wal-Mart objects to this request as overbroad, unduly burdensome, vague and ambiguous as to "any allegation that you have engaged in predatory pricing," not relevant to any party's claim or defense, disproportional to the needs of the case, and privileged under the attorney client and work product doctrines. Wal-Mart further objects to TPSA's definition of "document" because that definition includes some electronically stored information ("ESI") that is not reasonably accessible and would be unduly burdensome to retrieve and produce. Wal-Mart is withholding documents based on these objections.

Wal-Mart will not produce any additional documents in response to this request for production.

As became apparent from the argument at the hearing, it is Wal-Mart's view that the request is too broad and of such marginal relevance to even merit a search by Wal-Mart to find responsive documents. Having said that, it is also its view that there are likely to be responsive documents somewhere in its many offices and on its computer network, and that some of these documents would likely be privileged attorney client communications or work product. Thus, it stated that it was "withholding documents based on these objections." While that may technically be accurate, it is not what the new rules were after in adding the requirement in rule 34(b)(2)(C) that "an objection must state whether any responsive materials are being withheld on the basis of the objection." A more helpful response would have been something along the lines of "Based on these objections, Wal-Mart has not conducted a search for responsive documents, and while it is likely that some responsive documents may exist, Wal-Mart has not

Responding to Discovery Requests and Discovery Disputes

identified any such document, and is not withholding any identified document as a result of these objections."⁴⁷

Serving unsupported and boilerplate or stock objections does not preserve or accomplish anything other than waiver and subjecting the responding party to sanctions,⁴⁸ and "rule 26(g) 'and its commentary are starkly clear: an objection to requested discovery may not be made until after a lawyer has paused and consider[ed] whether, based on a reasonable inquiry, there is a factual [or legal] basis [for the] . . . objection."⁴⁹

General, boilerplate, and unsupported objections preserve nothing and—regardless of a party or an attorney's concerns about what they do not know or have not yet located or may later find—are "improper and ineffective."⁵⁰

The party resisting discovery must show specifically how each discovery request is not relevant or otherwise objectionable.⁵¹

And, although rule 26(b)(1) includes only "nonprivileged matter" within the proper scope of discovery⁵²—

When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial-prepara-

49. Heller, 303 F.R.D. at 477 (quoting Mancia, 253 F.R.D. at 358; internal quotation marks omitted).

50. Heller, 303 F.R.D. at 483-84.

51. See McLeod, Alexander, Powel & Apffel, P.C. v. Quarles, 894 F.2d 1482, 1485 (5th Cir. 1990); accord Innova Hosp. San Antonio, Ltd. P'ship v. Blue Cross & Blue Shield of Ga., Inc., 892 F.3d 719, 729 n.9 (5th Cir. 2018) ("While the Hospital did not file a motion to compel, this perhaps unadvised choice is not dispositive. Counsel have an obligation, as officers of the court, to assist in the discovery process by making diligent, good-faith responses to legitimate discovery requests."); McLeod, Alexander, Powel & Apffel, P.C. v. Quarles, 894 F.2d 1482, 1485–86 (5th Cir. 1990) (rejecting a party's contention that sanctions could not be imposed when the opposing party had not first requested an order to compel and stating that the party resisting discovery requests "must have a valid objection to each one in order to escape the production requirement"); Deutsche Bank National Trust Company v. Pink, No. 7:18-cv-20-O-BP, 2019 WL 399533, at *2 (N.D. Tex. Jan. 31, 2019); Hunt Construction Group, Inc. v. Cobb Mechanical Contractors, Inc., No. A-17-CV-215-LY, 2018 WL 5311380, at *3 (W.D. Tex. Oct. 25, 2018).

52. Fed. R. Civ. P. 26(b)(1).

^{47.} Wal-Mart Stores, Inc. v. Texas Alcoholic Beverage Commission, No. A-15-CV-134-RP, 2017 WL 1322247, at *1, *2 (W.D. Tex. Apr. 10, 2017).

^{48.} Hopkins v. Green Dot Corp., Civ. A. No. SA-16-CA-00365-DAE, 2016 WL 8673861, at *3 (W.D. Tex. Aug. 16, 2016) ("Courts consistently find waiver of a valid objection upon a party's use of boilerplate." (citing United States Sec. & Exch. Comm'n v. Commonwealth Advisors, Inc., No. CV31200700JWDEWD, 2016 WL 1364141, at *7 (M.D. La. Apr. 6, 2016) (collecting cases))).

tion material, the party must: (i) expressly make the claim; and (ii) describe the nature of the documents, communications, or tangible things not produced or disclosed—and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim.⁵³

Burden and Overbreadth: "If a discovery request is overbroad, the responding party must, to comply with . . . rule 34, explain the extent to which it is overbroad and answer or respond to the extent that it is not—and explain the scope of what the responding party is answering or responding to."⁵⁴

For example, if discovery is sought nationwide for a ten-year period, and the responding party objects on the grounds that only a five-year period limited to activities in the state of Florida is appropriate, the responding party shall provide responsive discovery falling within the five-year period as to the State of Florida.⁵⁵

And a party resisting discovery must show how the requested discovery is overly broad, unduly burdensome, or oppressive by submitting affidavits or offering evidence revealing the nature of the burden.⁵⁶ "Failing to do so, as a general matter, makes such an unsupported objection nothing more than unsustainable boilerplate."⁵⁷

So, "if answering or responding to a discovery request would impose an undue burden, the responding party must, as discussed below, properly substantiate that asser-

55. Consumer Electronics Ass'n v. Compras & Buys Magazine, Inc., No. 08-21085-CIV, 2008 WL 4327253, at *2 (S.D. Fla. Sept. 18, 2008).

56. See Deutsche Bank National Trust Company v. Pink, No. 7:18-cv-20-O-BP, 2019 WL 399533, at *3 (N.D. Tex. Jan. 31, 2019); CyWee Group Ltd. v. Samsung Electronics Co., Ltd., No. 2:17-CV-00140-RWS-RSP, 2018 WL 4112055, at *2 (E.D. Tex. Jan. 24, 2018); Vasquez v. Conquest Completion Services, LLC, No. MO:15-CV-188-DAE-DC, 2018 WL 3603069, at *2 (W.D. Tex. Jan. 10, 2018); Team Express Distributing, LLC v. Junction Solutions, Inc., No. SA-15-CA-00994-DAE, 2017 WL 10820159, at *1 (W.D. Tex. Aug. 30, 2017); Crownover v. Crownover, No. 2:15-CV-132-AM-CW, 2017 WL 10575859, at *2 (W.D. Tex. July 12, 2017); Merrill v. Waffle House, Inc., 227 F.R.D. 475, 477 (N.D. Tex. 2005); see also Robroy Industries-Texas, LLC v. Thomas & Betts Corporation, Nos. 2:15-CV-512-WCB & 2:16-CV-198-WCB, 2017 WL 319064 (E.D. Tex. Jan. 23, 2017) ("In the absence of some evidentiary showing that a discovery request would be burdensome, it is appropriate for a court to reject a request for a protective order on the ground that the undue burden claim is conclusory."); S.E.C. v. Brady, 238 F.R.D. 429, 437 (N.D. Tex. 2006) ("A party asserting undue burden typically must present an affidavit or other evidentiary proof of the time or expense involved in responding to the discovery request."); cf. JP Morgan Chase Bank, N.A. v. DataTreasury Corp., No. 18-40043, 2019 WL 3981305, at *6 n.6 (5th Cir. Aug. 23, 2019).

57. Heller, 303 F.R.D. at 490.

^{53.} Fed. R. Civ. P. 26(b)(5)(A).

^{54.} Heller, 303 F.R.D. at 488.

tion and then should only answer or respond to the part or extent, if any, of the request that would not involve an undue burden."⁵⁸

Vague and Ambiguous: A "party objecting to discovery as vague or ambiguous has the burden to show such vagueness or ambiguity" and "must explain the specific and particular way in which a request is vague."⁵⁹

"The responding party 'should exercise reason and common sense to attribute ordinary definitions to terms and phrases utilized in [discovery requests]. If necessary to clarify its answers [or responses], the responding party may include any reasonable definition of the term or phrase at issue.""⁶⁰

"Further, [i]f a party believes that the request is vague, that party [should] attempt to obtain clarification [by conferring with the requesting party] prior to objecting on this ground."⁶¹

Then, "if part or all of [a discovery request] is allegedly vague and ambiguous, the responding party, to comply with the federal rules, must, if possible, explain its understanding of the allegedly vague and ambiguous terms or phrases and explicitly state that its answer is based on that understanding."⁶²

In short, an objecting party bears a burden "to explain the specific and particular way that each request is . . . vague or ambiguous after exercising reason and common sense to attribute ordinary definitions to terms and phrases used in the request."⁶³ If an entire document request is truly so vague and ambiguous that the responding party cannot understand its meaning and what information it seeks, the party should stand on its objection and promise no production of responsive documents on the ground that the responding party simply cannot do so based on the discovery request's wording.⁶⁴

- 58. Heller, 303 F.R.D. at 489.
- 59. Heller, 303 F.R.D. at 491 (citations omitted).
- 60. Heller, 303 F.R.D. at 491 (citations omitted).

61. Heller, 303 F.R.D. at 491–92 (citations omitted); accord Casey v. Nationstar Mortgage, LLC, No. 1:14-CV-126-C, 2015 WL 11110966, at *2 (N.D. Tex. Feb. 5, 2015) ("Rule 34 requires that a party objecting to a discovery request explain its objection. Fed. R. Civ. P. 34(b)(2)(B) ('state an objection to the request, including the reasons') (emphasis added). Defendant did not state why any of these requests were vague, ambiguous, or non-specific in either its objections or its Response to the Plaintiffs' Motion.").

62. Heller, 303 F.R.D. at 488 (citations omitted).

63. Holcombe v. Advanced Integration Technology, No. 4:17-CV-522, 2018 WL 3819974, at *4 (E.D. Tex. Aug. 10, 2018).

"Subject to and without Waiving": Courts have recognized "that it has become common practice among many practitioners to respond to discovery requests by asserting objections and then answering 'subject to' or 'without waiving' their objections."⁶⁵ This practice "is inextricably intertwined with the related practice of raising boilerplate objections without the specificity that the federal rules require" and, "like the practice of including a stand-alone list of general or blanket objections that precede any responses to specific discovery requests[,] may have developed as a reflexive habit passed on from one attorney to another without any attorney giving serious thought or reflection as to what this manner of responding means or could hope to accomplish as to a particular discovery request."⁶⁶

But courts have now explained that—

- this practice of "responding to . . . documents requests 'subject to' and/or 'without waiving' objections is manifestly confusing (at best) and misleading (at worse), and has no basis at all in the Federal Rules of Civil Procedure";
- "this manner of responding to . . . [a document request] leaves the requesting party guessing and wondering as to the scope of the documents or information that will be provided as responsive will be";
- "outside of the privilege and work product context . . . , responding to . . . [a document request] 'subject to' and 'without waiving' objections is not consistent with the federal rules or warranted by existing law or by a non-frivolous argument for extending, modifying, or reversing existing law or for establishing new law";
- "a responding party has a duty to respond to or answer a discovery request to the extent that it is not objectionable" and "must describe what portions of [a document request] . . . it is, and what portions it is not, answering or responding to based on its objections and why";
- "if the request is truly objectionable—that is, the information or documents sought are not properly discoverable under the federal rules—the responding party should stand on an objection so far as it goes"; and

66. Heller, 303 F.R.D. at 486.

^{64.} See Heller, 303 F.R.D. at 488.

^{65.} Sprint Communications Co., L.P. v. Comcast Cable Communications, LLC, Nos. 11-2684-JWL, 11-2685-JWL, 11-2686-JWL, 2014 WL 545544, at *2 (D. Kan. Feb. 11, 2014).

"as a general matter, if an objection does not preclude or prevent a response or answer, at least in part, the objection is improper and should

And courts have explained that responding to documents requests "subject to" and/or "without waiving" objections, "without more, violate[s] the requirement of Fed. R. Civ. P. 34(b)(2)(C) that '[a]n objection must state whether any responsive materials are being withheld on the basis of that objection."⁶⁸

As one judge recently explained:

not be made."67

The practice of including "subject to" or "without waiving" statements after objections is an age-old habit comparable to belts and suspenders. This practice is "manifestly confusing (at best) and misleading (at worse), and has no basis at all in the Federal Rules of Civil Procedure." Such an objection and answer "leaves the requesting [p]arty uncertain as to whether the question has actually been fully answered," and "wondering as to the scope of the documents or information that will be provided as responsive."

The Court finds that Defendant's inclusion of "subject to and without waiving these objections" is not supported by the federal rules and goes against the purposes of a just, speedy, and inexpensive resolution. *See*

68. Source Network Sales & Marketing, LLC v. Jiangsu Mega Motor Company, No. 3:16-cv-1202-B-BK, 2017 WL 7596913, at *4 (N.D. Tex. Mey 15, 2017).

^{67.} Carr v. State Farm Mut. Auto. Ins. Co., 312 F.R.D. 459, 470 (N.D. Tex. 2015) (quoting Heller, 303 F.R.D. at 487-88); see also State Auto. Mat. Ins. Co. v. Freehold Mgmt., Inc., No. 3:16-cv-2255-L, 2018 WL 3548866, at *5 (N.D. Tex. July 24, 2018) (collecting cases); Parker v. Bill Melton Trucking, Inc., No. 3:15-cv-2528-G-BK, 2017 WL 6554139, at *2, *3 (N.D. Tex. Feb. 3, 2017) (explaining that "the all-too-common practice of responding to an inquiry 'subject to' or 'subject to and without waiving objection' is confusing and disfavored" and that "Plaintiff's use of the phrase 'subject to' makes it difficult to determine which documents she is withholding, and which she has agreed to produce"); Equal Employment Opportunity Commission v. Methodist Hospitals of Dallas, No. 3:15-cv-3104-G, 2016 WL 10703675, at *2 n.1 (N.D. Tex. Sept. 23, 2016) ("The undersigned continues to discourage litigants from responding to discovery requests that they have produced information 'subject to objection,' or 'without waiving objection.' Such responses only lead to confusion and 'busy work' for the Court, while reserving no substantive right. By the actual production of the materials, the right not to do so is necessarily waived. Also, such language does not preserve a subsequent objection to the use or admissibility of such materials, since an effective objection must be made at the time the material is actually offered as evidence."); Rivera v. United States, No. EP-15-CV-21-KC, 2015 WL 13649403, at *7 (W.D. Tex. Dec. 22, 2015) ("The Federal Rules of Civil Procedure do not allow a party to respond to discovery requests by stating objections and then answering the discovery request 'subject to and without waiving objections."").

Carr, 312 F.R.D. at 470. Further, by answering questions in such a manner Defendant fails to specify the scope of its answer in relation to the request. This makes it impossible for Plaintiffs or the Court to assess the sufficiency of the response.⁶⁹

And so courts have held that "[t]o make such an objection in the face of these considerations is to engage in the 'abusive practice of objecting to discovery requests reflexively—but not reflectively—and without a factual [or legal] basis' that [Federal Rule of Civil Procedure] 26(g) was enacted to stop."⁷⁰

Waiver of Objections: "[A]s a general rule, when a party fails to object timely to interrogatories, production requests, or other discovery efforts, objections thereto are waived."⁷¹

"If a party fails to timely respond in writing after being served with a request for production of documents, it is appropriate for the Court to find that the party's objections are waived, unless the court finds good cause and excuses [that] failure."⁷²

And, even where the responding party has timely served some objections to a rule 34(a) request, this waiver extends to any grounds not stated in a timely objection.⁷³

Timing of Responses and Objections: Federal Rule of Civil Procedure 34(b)(2)(A), as amended effective December 1, 2015, provides that "[t]he party to whom the [rule 34(a)] request is directed must respond in writing within 30 days after being served or—if the request was delivered under rule 26(d)(2)—within 30 days after the parties' first rule 26(f) conference" and that "[a] shorter or longer time may be stipulated to under rule 29 or be ordered by the court."⁷⁴ And Federal Rule of Civil Procedure 29 provides that—

^{69.} Halleen v. Belk, Inc., No. 4:16-CV-55, 2018 WL 3735579, at *3 (E.D. Tex. Aug. 6, 2018) (citations omitted).

^{70.} Heller, 303 F.R.D. at 487 (quoting Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354, 358 (D. Md. 2008)).

^{71.} In re United States, 864 F.2d 1153, 1156 (5th Cir. 1989).

^{72.} *Richmond v. SW Closeouts, Inc.*, No. 3:14-cv-4298-K, 2016 WL 3090672, at *5 (N.D. Tex. June 2, 2016); *accord Henderson v. Union Pac. R.R. Co.*, No. CV 15-0669, 2016 WL 5936889, at *2 (W.D. La. Oct. 11, 2016) ("Although rule 34 does not provide that untimely objections are waived, the Fifth Circuit has found that the waiver provision applies equally to rule 34." (citing *In re United States*, 864 F.2d at 1156)).

^{73.} See Fed. R. Civ. P. 34(b)(2)(B).

^{74.} Fed. R. Civ. P. 34(b)(1).

[u]nless the court orders otherwise, the parties may stipulate that: (a) a deposition may be taken before any person, at any time or place, on any notice, and in the manner specified—in which event it may be used in the same way as any other deposition; and (b) other procedures governing or limiting discovery be modified—but a stipulation extending the time for any form of discovery must have court approval if it would interfere with the time set for completing discovery, for hearing a motion, or for trial.⁷⁵

The federal rules thus provide that parties can agree to—or file a motion to ask the court for an order to—allow the responding party to serve written objections, responses, or answers and produce responsive materials in a period longer than thirty days.

A party who needs more time to respond or answer should ask for more time by explaining first to the requesting party—and, if necessary, to the court—what the responding party has done so far to search for and locate responsive information or documents and why it needs more time to answer or respond to some or all of the discovery requests and how much additional time it needs.

For example, while staged discovery or discovery in phases as contemplated in Federal Rule of Civil Procedure 26(f)(3)(B) may not be appropriate in a particular case, a party may be able to, within thirty days of the requests' service, serve written responses and produce documents in response to several requests that seek basic or readily accessible or identifiable information or materials, but may need to ask for an additional thirty or sixty days in which to serve written responses and—in some instances by a later specified date or on a rolling basis as contemplated in Federal Rule of Civil Procedure 34(b)(2)(B)—produce documents in response to other requests.

In the face of these rules, including rules 26(g)(1) and 26(g)(3)'s application to discovery responses and objections, the proper course for a party who needs more time to properly respond to discovery requests is not to ignore the thirty-day deadline (without a court order or agreement of the parties) or to serve general or boilerplate objections, but rather to seek more time to properly object or respond to or answer some or, if truly necessary, all of the discovery requests. Serving unsupported and boilerplate or stock objections is not a substitute for, or backdoor means of, requesting extensions of time to serve meaningful and supported objections and responses after further inquiry.⁷⁶ "General, boilerplate, and unsupported objections preserve nothing

75. Fed. R. Civ. P. 29.

and—regardless of a party or an attorney's concerns about what they do not know or have not yet located or may later find—are 'improper and ineffective."⁷⁷

"Neither is it appropriate to serve objections that a party or attorney has no factual basis for at the time of service but that the party or attorney is seeking to preserve for any responsive but objectionable materials or information that may later be found. Objections and responses and answers must be served based on what a reasonable inquiry presently shows."⁷⁸

"If additional or different materials or information are later uncovered, the proper course then is to comply with any supplementation obligations under Federal Rule of Civil Procedure 26(e)(1) and, if necessary, raise any appropriate objections for which there is, at that time, a legal and factual basis and to address the issue of why there is good cause to excuse the failure to have previously, timely raised the objections or seek leave to make the late objections for good cause."⁷⁹

§ 13.2:3 Federal Rule of Civil Procedure 37

Federal Rule of Civil Procedure 37(a) governs motions to compel discovery responses.

Rule 37(a)(3)(B) provides that a party seeking discovery may move for an order compelling production against another party when the latter has failed to produce documents requested under Federal Rule of Civil Procedure 34.⁸⁰ For purposes of rule 37(a), "an evasive or incomplete disclosure, answer, or response must be treated as a failure to disclose, answer, or respond."⁸¹

^{76.} See, generally, Heller, 303 F.R.D. at 477.

^{77.} Lopez v. Don Herring Ltd., 327 F.R.D. 567, 583 (N.D. Tex. 2018) (Heller, 303 F.R.D. at 483–84).

^{78.} Lopez, 327 F.R.D. at 583.

^{79.} Lopez, 327 F.R.D. at 583.

^{80.} See Fed. R. Civ. P. 37(a)(3)(B)(iv); accord Crosswhite v. Lexington Ins. Co., 321 F. App'x 365, 368 (5th Cir. 2009) ("A party may move to compel production of materials that are within the scope of discovery and have been requested but not received. Fed. R. Civ. P. 37(a). Yet, a court may decline to compel, and, at its option or on motion, 'may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden . . . , including . . . forbidding inquiry into certain matters, or limiting the scope of disclosure or discovery to certain matters.' Fed. R. Civ. P. 26(c)(1)(D); see also Fed. R. Civ. P. 37(a)(5)(B).").

^{81.} Fed. R. Civ. P. 37(a)(4).

Conversely, a party served with discovery requests for ESI may move for a protective order under Federal Rule of Civil Procedure 26(c). Rule 26(c)(1) provides that—

[a] party or any person from whom discovery is sought may move for a protective order in the court where the action is pending-or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken. The motion must include a certification that the movant has in good faith conferred or attempted to confer with other affected parties in an effort to resolve the dispute without court action. The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following: (A) forbidding the disclosure or discovery; (B) specifying terms, including time and place or allocation of expenses, for the disclosure or discovery; (C) prescribing a discovery method other than the one selected by the party seeking discovery; (D) forbidding inquiry into certain matters, or limiting the scope of disclosure or discovery to certain matters; (E) designating the persons who may be present while the discovery is conducted; (F) requiring that a deposition be sealed and opened only on court order; (G) requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way; and (H) requiring that the parties simultaneously file specified documents or information in sealed envelopes, to be opened as the court directs.⁸²

Under rule 26(c)(2), "[i]f a motion for a protective order is wholly or partly denied, the court may, on just terms, order that any party or person provide or permit discovery."⁸³

Courts have held that, once responses, answers, and objections have been served subject to rule 26(g), the party who has objected to a discovery request then must, in response to a rule 37(a) motion to compel or in support of its own Federal Rule of Civil Procedure 26(c) motion for a protective order, urge and argue in support of its objection to an interrogatory or request, and, if it does not, it waives the objection.⁸⁴

^{82.} Fed. R. Civ. P. 26(c)(1).

^{83.} Fed. R. Civ. P. 26(c)(2).

^{84.} See Orchestratehr, Inc. v. Trombetta, 178 F. Supp. 3d 476, 507 (N.D. Tex. 2016) (citing Dolquist v. Heartland Presbytery, 221 F.R.D. 564, 568 (D. Kan. 2004); Cotracom Commodity Trading Co. v. Seaboard Corp., 189 F.R.D. 655, 662 (D. Kan. 1999)).

Of course, a party "cannot produce what it does not have," and so "[c]learly, the court cannot compel [a party] to produce non-existent documents."⁸⁵

Although Federal Rule of Civil Procedure 26(b) has been amended, effective December 1, 2015, the amendments to rule 26 do not alter the burdens imposed on the party resisting discovery discussed above.⁸⁶

The governing case law in the Fifth Circuit provides that, even if certain discovery requests seek irrelevant information or materials, the party resisting discovery "must have a valid objection to each one in order to escape the production requirement" and that the party resisting discovery must show specifically how each request is not relevant or otherwise objectionable as, for example, overly broad, burdensome, or oppressive.⁸⁷

And the United States Court of Appeals for the Fifth Circuit has long held that, under rule 26(c)(1), "'[t]he burden is upon [the party seeking the protective order] to show the necessity of its issuance, which contemplates a particular and specific demonstration of fact as distinguished from stereotyped and conclusory statements."⁸⁸ A protective order is warranted in those instances in which the party seeking it demonstrates good cause and a specific need for protection.⁸⁹

The combined effect of these rules and standards has been to place the burden on the party resisting discovery to show that the requested discovery does not fall within rule 26(b)(1)'s scope of proper discovery—often referred to in shorthand as "relevance" for purposes of discovery—or that a discovery request would impose an undue burden or expense, including one that outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

Just as was the case before the December 1, 2015, amendments, under rules 26(b)(1) and 26(b)(2)(C)(iii), "a court can—and must—limit proposed discovery that it deter-

^{85.} ORIX USA Corp. v. Armentrout, No. 3:16-mc-63-N-BN, 2016 WL 4095603, at *5 (N.D. Tex. Aug. 1, 2016) (collecting cases).

^{86.} See Carr, 312 F.R.D. at 463-69.

^{87.} McLeod, 894 F.2d at 1485.

^{88.} In re Terra Int'l, 134 F.3d 302, 306 (5th Cir. 1998) (quoting United States v. Garrett, 571 F.2d 1323, 1326 n.3 (5th Cir. 1978)).

^{89.} See Landry v. Air Line Pilots Ass'n, 901 F.2d 404, 435 (5th Cir. 1990).

mines is not proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit—and the court must do so even in the absence of a motion."⁹⁰

"But the amendments to rule 26(b) and rule 26(c)(1) do not alter the basic allocation of the burden on the party resisting discovery to—in order to prevail on a motion for protective order or successfully resist a motion to compel—specifically object and show that the requested discovery does not fall within rule 26(b)(1)'s scope of proper discovery (as now amended) or that a discovery request would impose an undue burden or expense or is otherwise objectionable."⁹¹

Thus, as amended, rule 26(b)(2)(C) provides that, "[o]n motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or (iii) the proposed discovery is outside the scope permitted by rule 26(b)(1)."⁹²

[U]nder Fifth Circuit law, the party resisting discovery must show specifically how each discovery request is not relevant or otherwise objectionable. That is true on a rule 37(a) motion to compel no less than on a [Federal Rule of Civil Procedure] 26(c) motion for a protective order.

. . . .

Rule 26(g)(1) does not impose on a party filing a motion to compel the burden to show relevance and proportionality in the first instance.

[And] rule 26(b)(1) does not place on the party seeking discovery the burden of addressing all proportionality considerations. While it is a good

^{90.} Lopez v. Don Herring Ltd., 327 F.R.D. 567, 583 (N.D. Tex. 2018) (citing Crosby v. La. Health Serv. & Indem. Co., 647 F.3d 258, 264 (5th Cir. 2011)); see also JP Morgan Chase Bank, N.A. v. DataTreasury Corp., No. 18-40043, 2019 WL 3981305, at *6 (5th Cir. Aug. 23, 2019).

^{91.} Carr v. State Farm Mut. Auto. Ins. Co., 312 F.R.D. 459, 468 (N.D. Tex., 2015) (citing McLeod, 894 F.2d at 1485; Heller, 303 F.R.D. at 483–93); accord Vallejo v. Amgen, Inc., 903 F.3d 733, 742 (8th Cir. 2018) (quoting Carr, 312 F.R.D. at 468).

^{92.} Fed. R. Civ. P. 26(b)(2)(C).

practice for a movant to explain the relevance and proportionality of its discovery requests, and while a failure to appropriately address rule 26(b)(1) proportionality factors may be determinative in a proportionality analysis and result in the motion to compel being denied on its merits, [t]he parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes.⁹³

Samsung Electronics America, Inc. v. Chung, 325 F.R.D. 578, 594–95 (N.D. Tex. 2017) (citations omitted).

The existing allocation of burdens to show undue burden or lack of proportionality have not fundamentally changed after December 1, 2015.⁹⁴

A party seeking to resist discovery on rule 26(b)(1) and rule 26(b)(2)(C)(iii) grounds still bears the burden of making a specific objection and showing that any discovery request that is relevant to any party's claim or defense fails the proportionality calculation mandated by rule 26(b) by coming forward with specific information to address—insofar as that information is available to it—the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.⁹⁵

The party seeking discovery, as noted above, may well—to prevail on a motion to compel—need to make its own showing of many or all of the proportionality factors, including the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to rele-

^{93.} Accord Charalambopoulos v. Grammar, No. 3:14-cv-2424-D, 2017 WL 1094394, at *4 n.5 (N.D. Tex. Mar. 8, 2017).

^{94.} Carr, 312 F.R.D. at 466.

^{95.} Lopez, 327 F.R.D. at 584; see also Deutsche Bank National Trust Company v. Pink, No. 7:18cv-20-O-BP, 2019 WL 399533, at *2, *5 (N.D. Tex. Jan. 31, 2019); accord First Am. Bankcard, Inc. v. Smart Bus. Tech., Inc., No. CV 15-638, 2017 WL 2267149, at *1 (E.D. La. May 24, 2017) ("In this instance, defendant has offered nothing more than a boilerplate proportionality objection, without providing any information concerning burden or expense that the court would expect to be within defendant's own knowledge."); Parker v. Bill Melton Trucking, Inc., No. 3:15-cv-2528-G-BK, 2017 WL 6554139, at *1 (N.D. Tex. Feb. 3, 2017) ("A party resisting discovery on the grounds that it fails the proportionality calculation bears the burden of coming forth with specific information to address the proportionality considerations outlined in rule 26(b)(1).").

vant information, the parties' resources, and the importance of the discovery in resolving the issues, in opposition to the resisting party's showing.⁹⁶

And, the party seeking discovery is required in the first instance to comply with rule 26(b)(1)'s proportionality limits on discovery requests; is subject to Federal Rule of Civil Procedure 26(g)(1)'s requirement to certify that—

to the best of the person's knowledge, information, and belief formed after a reasonable inquiry . . . with respect to a discovery request . . . , it is: (i) consistent with these rules and warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law, or for establishing new law; (ii) not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and (iii) neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action"; and faces rule 26(g)(3) sanctions "[i] f a certification violates this rule without substantial justification."⁹⁷

But the amendments to rule 26(b) do not alter the basic allocation of the burden on the party resisting discovery to—in order to successfully resist a motion to compel—specifically object and show that the requested discovery does not fall within rule 26(b)(1)'s scope of relevance (as now amended) or fails the required proportionality calculation or is otherwise objectionable.⁹⁸

Courts have also explained that "a proper rule 37(a) motion to compel . . . must include a certification that the movant has made a good faith effort to meet and confer regarding the specific discovery disputes at issue, and to resolve them without court intervention, as required by Federal Rule of Civil Procedure 37(a)(1)."⁹⁹

When a motion to compel addresses a number of matters, a good faith effort to confer typically requires that the parties discuss each matter in good faith to comply with conference requirements. When it may require

^{96.} Lopez, 327 F.R.D. at 584.

^{97.} Fed. R. Civ. P. 26(g)(1)(B), 26(g)(3); see generally Heller, 303 F.R.D. at 475-77, 493-95.

^{98.} Lopez, 327 F.R.D. at 584 (citing McLeod, 894 F.2d at 1485; Heller, 303 F.R.D. at 483–93); see also Hunt Construction Group, Inc. v. Cobb Mechanical Contractors, Inc., No. A-17-CV-215-LY, 2018 WL 5311380, at *3, *4 (W.D. Tex. Oct. 25, 2018); Samsung Electronics America Inc. v. Chung, 325 F.R.D. 578, 591–92 (N.D. Tex. 2017).

^{99.} Samsung, 321 F.R.D. at 285.

several hours of court time to resolve the numerous issues raised, it seems logical that the parties will have spent an equal or greater amount of time attempting to resolve the issues without judicial involvement.¹⁰⁰

A proper rule 37(a) motion to compel also "must attach a copy of the discovery requests at issue (such as rule 34 requests for production or inspection, rule 33 interrogatories, a transcript of deposition testimony, deposition notice, or subpoena) and of the resisting party's responses and objections to those requests; must specifically and individually identify each discovery request in dispute and specifically, as to each request, identify the nature and basis of the dispute, including, for example, explaining ... how a response or answer is deficient or incomplete, and ask the Court for specific relief as to each request; and must include a concise discussion of the facts and authority that support the motion as to each discovery request in dispute."¹⁰¹

Federal Rule of Civil Procedure 37(a)(5)(A) provides that if a motion to compel is granted or if the requested discovery is provided after the motion was filed, "the court must, after giving an opportunity to be heard, require the party . . . whose conduct necessitated the motion, the party or attorney advising that conduct, or both to pay the movant's reasonable expenses incurred in making the motion, including attorney's fees," except that "the court must not order this payment if: (i) the movant filed the motion before attempting in good faith to obtain the disclosure or discovery without court action; (ii) the opposing party's nondisclosure, response, or objection was substantially justified; or (iii) other circumstances make an award of expenses unjust."¹⁰²

Federal Rules of Civil Procedure 37(a)(5)(B) and 37(a)(5)(C) further provide in pertinent part that, "[i]f the motion is denied, the court may issue any protective order authorized under rule 26(c) and must, after giving an opportunity to be heard, require the movant, the attorney filing the motion, or both to pay the party . . . who opposed the motion its reasonable expenses incurred in opposing the motion, including attorney's fees," "[b]ut the court must not order this payment if the motion was substantially justified or other circumstances make an award of expenses unjust," and that

^{100.} Brown v. Bridges, No. 12-cv-4947-P, 2015 WL 1 1121361, at *4 (N.D. Tex. Jan. 30, 2015) (citation omitted).

^{101.} Samsung, 325 F.R.D. at 594–95 (quoting Harrison v. Wells Fargo Bank, N.A., No. 3:13-cv-4682-D, 2016 WL 1392332, at *7 (N.D. Tex. Apr. 8, 2016) (citing Fed. R. Civ. P. 7(b)(1); Fed. R. Civ. P. 37(a); N.D. Tex. L. Civ. R. 5.2(3); N.D. Tex. L. Civ. R. 7.1).

^{102.} Fed. R. Civ. P. 37(a)(5)(A); accord Washington v. M. Hanna Const. Inc., 299 F. App'x 399, 402 (5th Cir. 2008).

"[i]f the motion is granted in part and denied in part, the court may issue any protective order authorized under rule 26(c) and may, after giving an opportunity to be heard, apportion the reasonable expenses for the motion."¹⁰³

Federal Rule of Civil Procedure 26(c)(3) provides that in connection with a motion under rule 26(c) for a protective order, Federal Rule of Civil Procedure "37(a)(5) applies to the award of expenses."¹⁰⁴

"[A] motion is 'substantially justified' if there is a genuine dispute, or if reasonable people could differ as to [the appropriateness of the contested action]."¹⁰⁵

§ 13.2:4 Federal Rule of Civil Procedure 45

"Federal Rule of Civil Procedure 45 'explicitly contemplates the use of subpoenas in relation to nonparties' and governs subpoenas served on a third party . . . as well as motions to quash or modify or to compel compliance with such a subpoena."¹⁰⁶

Rule 45 provides certain specific rules as to the form of production of ESI,¹⁰⁷ but otherwise, as with the federal rules governing discovery from a party, the federal rules do not provide special rules for requests for ESI from nonparties. The rules for serving discovery for ESI on nonparties are more fully discussed elsewhere in this volume.

Once "properly served with a rule 45 subpoena, a nonparty is subject to discovery obligations that the subpoena imposes, as limited by rule 45's protections that the nonparty is entitled to invoke."¹⁰⁸ To invoke those protections through objections, rule 45(d)(2) requires that the subpoenaed party "serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested."¹⁰⁹

107. See Fed. R. Civ. P. 45(a)(1)(C), (e)(1).

108. Andra Group, LP v. JDA Software Group, Inc., No. 3:15-mc-11-K-BN, 2015 WL 1636602, at *6 (N.D. Tex. Apr. 13, 2015).

109. Fed. R. Civ. P. 45(d)(2)(B).

^{103.} Fed. R. Civ. P. 37(a)(5)(B)–(C); accord De Angelis v. City of El Paso, 265 F. App'x 390, 398 (5th Cir. 2008).

^{104.} Fed. R. Civ. P. 26(c)(3).

^{105.} De Angelis, 265 F. App'x at 398; see also Heller, 303 F.R.D. at 477.

^{106.} Am. Fed'n of Musicians of the U.S. & Canada v. SKODAM Films, LLC, 313 F.R.D. 39, 42 (N.D. Tex. 2015) (quoting Isenberg v. Chase Bank USA, N.A., 661 F. Supp. 2d 627, 629 (N.D. Tex. 2009)).

Federal Rule of Civil Procedure 45(a)(1)(C) provides that "[a] command to produce documents, electronically stored information, or tangible things . . . may be included in a subpoena commanding attendance at a deposition."¹¹⁰ And Federal Rule of Civil Procedure 45(d)(2)(A) directs that "[a] person commanded to produce documents, electronically stored information, or tangible things . . . need not appear in person at the place of production . . . unless also commanded to appear for a deposition, hearing, or trial."¹¹¹

Under Federal Rule of Civil Procedure 45(d)(1), "[a] party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena," and "[t]he court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply."¹¹²

And Federal Rule of Civil Procedure 45(d)(2)(B) requires that "[a] person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested"—and that "[t]he objection must be served before the earlier of the time specified for compliance or fourteen days after the subpoena is served."¹¹³

Under rule 45(d)(2)(B)—

[if] an objection is made, the following rules apply: (i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection. (ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.¹¹⁴

114. Fed. R. Civ. P. 45(d)(2)(B).

^{110.} Fed. R. Civ. P. 45(a)(1)(C).

^{111.} Fed. R. Civ. P. 45(d)(2)(A).

^{112.} Fed. R. Civ. P. 45(d)(1); see also Am. Fed'n of Musicians of the U.S. & Canada v. SKODAM Films, LLC, 313 F.R.D. 39, 57–59 (N.D. Tex. 2015).

^{113.} Fed. R. Civ. P. 45(d)(2)(B).

third party to comply with a rule 45(a) subpoena.

Courts have also held that "a nonparty's rule 45(d)(2)(B) objections to discovery requests in a subpoena are subject to the same prohibition on general or boilerplate [or unsupported] objections and requirements that the objections must be made with specificity and that the responding party must explain and support its objections."¹¹⁶ According to this interpretation of the rules, just as "[a]lthough [Federal Rule of Civil Procedure] 34 governs document discovery from a party and not a nonparty, see Fed. R. Civ. P. 34(c)," "Rule 34(b)(1)'s reasonable particularity requirement should apply with no less force to a subpoena's document requests to a nonparty," so too "a nonparty's rule 45(d)(2)(B) objections to those requests should be subject to the same requirements facing a party objecting to discovery under rule 34."¹¹⁷

This means (1) that a nonparty is subject to the requirements that an objection to a document request must, for each item or category, state with specificity the grounds for objecting to the request, including the reasons, and must state whether any responsive materials are being withheld on the basis of that objection; (2) that an objection to part of a request must specify the part and permit inspection of the rest; (3) that "general or so-called boilerplate or unsupported objections are improper under rule 45(d)(2)(B)"; and (4) the requirements to make proper objections and how to properly respond to discovery requests apply equally to nonparties subject to a rule 45 subpoena.¹¹⁸

Under Federal Rule of Civil Procedure 45(d), "[e]ither in lieu of or in addition to serving objections on the party seeking discovery, a person can 'timely' file a motion to quash or modify the subpoena" under Federal Rule of Civil Procedure 45(d)(3)(A).¹¹⁹ Under rule 45(d)(3)(A), "[o]n timely motion, the court for the district where compli-

^{115.} See Fed. R. Civ. P. 45(d)(2)(B)(ii); Am. Fed'n, 313 F.R.D. at 44.

^{116.} *Am. Fed'n*, 313 F.R.D. at 46 (citing *Heller v. City of Dallas*, 303 F.R.D. 466, 483 (N.D. Tex. 2004), and adopting "the explanations in *Heller* of what is required to make proper objections and how to properly respond to discovery requests").

^{117.} Am. Fed'n, 313 F.R.D. at 44, 46.

^{118.} See Am. Fed'n, 313 F.R.D. at 46; Fed. R. Civ. P. 34(b)(2)(B)-(C).

^{119.} In re Ex Parte Application of Grupo Mexico SAB de CV, No. 3:14-mc-73-G, 2015 WL 12916415, at *3 (N.D. Tex. Mar. 10, 2015), aff'd sub nom. Grupo Mexico SAB de CV v. SAS Asset Recovery, Ltd., 821 F.3d 573 (5th Cir. 2016).

ance is required must quash or modify a subpoena that (i) fails to allow a reasonable time to comply; (ii) requires a person to comply beyond the geographical limits specified in rule 45(c); (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or (iv) subjects a person to undue burden.¹²⁰

And, "[i]n the majority of cases, a person—whether a traditional party (i.e., a plaintiff or defendant) or a nonparty—waives objections if he/she/it fails either to serve timely objections on the party seeking discovery or to file a timely motion with the court."¹²¹

As one judge in the Fifth Circuit has explained:

When a nonparty to a lawsuit . . . is served with an overly broad subpoena duces tecum, . . . the nonparty has four procedural options. First, it may ignore the subpoena. This is the worst option, almost certain to result in a contempt citation under rule 45(g) and a finding that all objections have been waived. Second, the nonparty may comply with the subpoena, an option that appears to be less frequently chosen in these contentious times.

Third, the nonparty "*may* serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested." Fed. R. Civ. P. 45(d)(2)(B) (emphasis added). Significantly, this rule uses the permissive "may." It does not use the mandatory "shall" or "must." The non-party is not required to serve written objections. Instead, serving written objections is a less formal, easier, usually less expensive method of fore-stalling subpoena compliance when compared to the separate option of filing a motion to quash or modify the subpoena, as discussed below. However, if the subpoena recipient chooses to serve written objections must be served on the issuing party "before the earlier of the time specified for compliance or 14 days after the subpoena is served."

Serving written objections under rule 45(d)(2)(B) may provide the recipient with several advantages. For example, asserting objections can be done

^{120.} Fed. R. Civ. P. 45(d)(3)(A).

^{121.} *Grupo Mexico*, 2015 WL 12916415, at *3; *accord Am. Fed'n*, 313 F.R.D. at 43 (explaining that "[t]he failure to serve written objections to a subpoena within the time specified by rule [45(d)(2)(B)] typically constitutes a waiver of such objections, as does failing to file a timely motion to quash.").
informally without going to court, shifts the burden and expense of commencing motion practice in court to the issuing party and affords the recipient additional time in the event the recipient is ultimately obligated to comply with the demands in the subpoena.

The nonparty's fourth option is the one that [the nonparty] elected to exercise in this case. Under rule 45(d)(3), the subpoena recipient may move to modify or quash the subpoena as a means of asserting its objections to the subpoena. Unlike serving rule 45(d)(2)(B) written objections, a motion to quash is not subject to the fourteen-day requirement. Instead, the rule provides simply that the motion to quash must be "timely." Fed. R. Civ. P. 45(d)(3)(A). As the leading commentators and the case law they rely upon explain, the "fourteen-day requirement to object to a subpoena is not relevant to a motion to quash a subpoena . . ." Wright & Miller (emphasis added) and cases cited at n.10, including COA Inc. v. Xiamei Houseware Group Co., Inc., No. C13-771 MJP, 2013 WL 2332347, *2 (W.D. Wash. May 28, 2013) (quoting King v. Fidelity Nat. Bank of Baton Rouge, 712 F.2d 188, 191 (5th Cir. 1983)); In re Kulzer, No. 3:09-MC-08 CAN, 2009 WL 961229 (N.D. Ind. Apr. 8, 2009), rev'd on other grounds Heraeus Kulzer, GmbH v. Biomet, Inc., 633 F.3d 591 (7th Cir. 2011) (motion to quash was timely even though it was not served within fourteen-day time limit).

Rules 45(d)(2) and 45(d)(3) provide a nonparty subpoena recipient with two separate and distinct procedural vehicles for asserting objections to a subpoena. One is not dependent upon or tied to the other. One must be filed within fourteen days of receipt; the other must merely be "timely," ordinarily meaning filed before the date set in the subpoena for compliance.¹²²

On a rule 45(d)(3)(A) motion to quash or modify a subpoena, the moving party has the burden of proof.¹²³ And, "[g]enerally, modification of a subpoena is preferable to quashing it outright."¹²⁴

^{122.} Arthur J. Gallagher & Co. v. O'Neill, No. 17-2825, 2017 WL 5713361, at *1, *2, *4 (E.D. La. Nov. 27, 2017) (emphasis in original; citation omitted); accord Monitronics Int'l, Inc. v. iControl Networks, Inc., No. 3:13-mc-134-L-BN, 2013 WL 6120540, at *1 (N.D. Tex. Nov. 21, 2013) ("Rule 45 does not define a 'timely motion' but does provide that, if the subpoenaed party chooses to serve objections instead of moving to quash, '[t]he objection must be served before the earlier of the time specified for compliance or fourteen days after the subpoena is served.' Fed. R. Civ. P. 45(c)(2)(B).").

^{123.} See Wiwa v. Royal Dutch Petroleum Co., 392 F.3d 812, 818 (5th Cir. 2004); Williams v. City of Dallas, 178 F.R.D. 103, 109 (N.D. Tex. 1998).

^{124.} Wiwa, 392 F.3d at 818.

On a motion asserting undue burden, "[t]he moving party has the burden of proof to demonstrate 'that compliance with the subpoena would be unreasonable and oppressive."¹²⁵ "The moving party opposing discovery must show how the requested discovery was overly broad, burdensome, or oppressive by submitting affidavits or offering evidence revealing the nature of the burden."¹²⁶

"Whether a burdensome subpoena is reasonable must be determined according to the facts of the case, such as the party's need for the documents and the nature and importance of the litigation."¹²⁷ "To determine whether the subpoena presents an undue burden, [the Court] consider[s] the following factors: (1) relevance of the information requested; (2) the need of the party for the documents; (3) the breadth of the document request; (4) the time period covered by the request; (5) the particularity with which the party describes the requested documents; and (6) the burden imposed."¹²⁸ "Further, if the person to whom the document request is made is a nonparty, the court may also consider the expense and inconvenience to the nonparty."¹²⁹

And, when "a subpoena is issued as a discovery device, relevance for purposes of the undue burden test is measured according to the standard of [Federal Rule of Civil Procedure] 26(b)(1)."¹³⁰ This is because discovery from a third party as permitted through a subpoena issued under rule 45 is limited to the scope of discovery permitted under rule 26(b)(1) in the underlying action, and "[d]iscovery outside of this scope is not permitted."¹³¹ The provisions and structure of rules 26 and 45 leave little doubt that

127. Wiwa, 392 F.3d at 818 (footnote omitted).

128. Wiwa, 392 F.3d at 818 (footnote omitted).

129. Wiwa, 392 F.3d at 818 (footnote omitted); accord Positive Black Talk Inc. v. Cash Money Records, Inc., 394 F.3d 357, 377 (5th Cir. 2004), abrogated on other grounds by Reed Elsevier, Inc., v. Muchnick, 559 U.S. 154 (2010) ("Fed. R. Civ. P. 45 provides that a court shall quash (or modify) a subpoena if it 'subjects a person to undue burden.' Fed. R. Civ. P. 45(c)(3)(A)(iv). Whether a subpoena subjects a witness to undue burden generally raises a question of the subpoena's reasonableness, which 'requires a court to balance the interests served by demanding compliance with the subpoena against the interests furthered by quashing it.' 9A Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure, § 2463 (2d ed. 1995). '[T]his balance of the subpoena's benefits and burdens calls upon the court to consider whether the information is necessary and unavailable from any other source.'").

130. Williams, 178 F.R.D. at 110.

131. Garcia v. Professional Contract Servs., Inc., No. A-15-cv-585-LY, 2017 WL 187577, at *2 (W.D. Tex. Jan. 17, 2017); see also Arthur J. Gallagher & Co., 2017 WL 5713361, at *2 (explaining that "subpoenas duces tecum are discovery devices governed by rule 45 but also subject to the parameters established by rule 26" and that a "court retains discretion to decline to compel production of requested documents when the request exceeds the bounds of fair discovery, even if a timely objection has not been made").

^{125.} Wiwa, 392 F.3d at 818 (quoting Williams, 178 F.R.D. at 109.

^{126.} Andra Group, LP v. JDA Software Group, Inc., 312 F.R.D. 444, 449 (N.D. Tex. 2015).

the scope of permissible discovery from a third party is not broader than that permitted against a party.¹³²

Because "[t]he scope of discovery is the same under both Federal Rules of Civil Procedure 45 and 26,"¹³³ courts apply the rule 26(b)(1) proportionality factors in the context of a rule 45(d)(3)(A) motion to quash or a rule 45(d)(2)(B)(i) motion to compel or, for that matter, in the context of rule 45(d)(1)'s duty to avoid imposing undue burden or expense on a person subject to the subpoena.¹³⁴ And, as one judge in the Fifth Circuit has noted, where "nonparties have greater protections from discovery," "burdens on nonparties will impact the proportionality analysis."¹³⁵

The Court also "may find that a subpoena presents an undue burden when the subpoena is facially overbroad."¹³⁶ "Courts have found that a subpoena for documents from a nonparty is facially overbroad where the subpoena's document requests 'seek all documents concerning the parties to [the underlying] action, regardless of whether those documents relate to that action and regardless of date;' '[t]he requests are not particularized;' and '[t]he period covered by the requests is unlimited."¹³⁷

135. Hume v. Consolidated Grain & Bargε, Inc., Civ. A. No. 15-935, 2016 WL 7385699, at *3 (E.D. La. Dec. 21, 2016) (quoting E. Laporte and J. Redgrave, A Practical Guide to Achieving Proportionality Under New Federal Rule of Civil Procedure 26, 9 Fed. Cts. L. Rev. 19, 57 (2015)).

136. Wiwa, 392 F.3d at 818 (footnote omitted).

137. Am. Fed'n, 313 F.R.D. at 45.

^{132.} See Waters v. Lincoln Gen'l Ins. Co., Civ. A. No. 07-3183, 2008 WL 659471, at *2 (E.D. La. Mar. 5, 2008) ("The scope of discovery with respect to nonparties under rule 45 is no broader than that prescribed for parties under rule 26(b)(1)."); accord Wiwa, 392 F.3d at 818 ("Further, if the person to whom the document request is made is a nonparty, the court may also consider the expense and inconvenience to the nonparty." (footnote omitted) (citing Williams, 178 F.R.D. at 109 ("The status of a witness as a nonparty entitles the witness to consideration regarding expense and inconvenience."), which cited Concord Boat Corp. v. Brunswick Corp., 169 F.R.D. 44, 49 (S.D.N.Y. 1996) ("In addition, the status of a witness as a nonparty to the underlying litigation 'entitles [the witness] to consideration regarding expense and inconvenience.""), which cited Fed. R. Civ. P. 45(c)(2)(B) and Semtek Int'l, Inc. v. Merkuriy Ltd., No. 3607 DRH, 1996 WL 238538, at *2 (N.D.N.Y. May 1, 1996) ("Second, Lockheed is a nonparty. While this status does not relieve Lockheed of its obligations either to respond to proper discovery requests or to comply with the applicable rules, it does entitle Lockheed to consideration regarding expense and inconvenience."))); cf. Am. Fed'n, 313 F.R.D. at 45 ("The Court finds that applying the standards of rule 26(b)(1), as amended, to the Subpoena and [the plaintiff's] motion to compel is both just and practicable where [a party] is not entitled to enforce its Subpoena against a nonparty based on a greater scope of relevance than should apply tc any discovery against any party going forward.").

^{133.} Garcia, 2017 WL 187577, at *2.

^{134.} See Am. Fed'n, 313 F.R.D. at 44-45.

§ 13.3

§ 13.3 Texas State Court

The Texas Rules of Civil Procedure control the scope of a proper discovery request for ESI and how to properly respond to a request.

§ 13.3:1 Texas Rule of Civil Procedure 196.4

The Texas Rules include a specific rule governing requests for ESI:

To obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced. The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If the responding party cannot—through reasonable efforts—retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules. If the court orders the responding party to comply with the request, the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.¹³⁸

"This rule's focus on production of data that is 'reasonably available' in the 'ordinary course of business' with 'reasonable efforts' reflects a policy underlying discovery in general—and electronic discovery in particular—to achieve an appropriate balance between discoverability and accompanying burdens."¹³⁹ This is further reflected in Texas Rule of Civil Procedure 192.4, which provides that—

[t]he discovery methods permitted by these rules should be limited by the court if it determines, on motion or on its own initiative and on reasonable notice, that:

(a) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; or

^{138.} Tex. R. Civ. P. 196.4.

^{139.} In re Methodist Primary Care Group, 553 S.W.3d 709, 715 (Tex. App.—Houston [14th Dist.], 2018, orig. proceeding).

(b) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.¹⁴⁰

The Texas Supreme Court's decision in "*In re Weekley Homes, L.P.*, 295 S.W.3d [309,] 315–22 [(Tex. 2009)], sets forth the procedures for obtaining discovery of electronic information under Texas Rule of Civil Procedure 196.4," under which the Supreme Court "summarized the proper procedures . . . as follows:

- 'When a specific request for electronic information has been lodged, rule 196.4 requires the responding party to either produce responsive electronic information that is 'reasonably available to the responding party in its ordinary course of business,' or object on grounds that the information cannot through reasonable efforts be retrieved or produced in the form requested.'
- 'Once the responding party raises a rule 196.4 objection, either party may request a hearing at which the responding party must present evidence to support the objection. Tex. R. Civ. P. 193.4(a).'
- 'To determine whether requested information is reasonably available in the ordinary course of business, the trial court may order discovery, such as requiring the responding party to sample or inspect the sources potentially containing information identified as not reasonably available.'
- 'Should the responding party fail to meet its burden, the trial court may order production subject to the discovery limitations imposed by rule 192.4.'
- 'If the responding party meets its burden by demonstrating that retrieval and production of the requested information would be overly burdensome, the trial court may nevertheless order targeted production upon a showing by the requesting party that the benefits of ordering production outweigh the costs. Tex. R. Civ. P. 192.4.'

140. Tex. R. Civ. P. 192.4.

• 'To the extent possible, courts should be mindful of protecting sensitive information and should choose the least intrusive means of retrieval.'"¹⁴¹

The Texas Supreme Court later explained in *In re State Farm Lloyds*, 520 S.W.3d 595 (Tex. 2017), that, "[t]hough the term 'reasonable' cannot be comprehensively defined, it naturally invokes the jurisprudential considerations articulated in rule 192.4":¹⁴²

- "Thus, if the responding party objects that electronic data cannot be retrieved in the form requested through 'reasonable efforts' and asserts that the information is readily 'obtainable from some other source that is more convenient, less burdensome, or less expensive,' the trial court is obliged to consider whether production in the form requested should be denied in favor of a 'reasonably usable' alternative form."¹⁴³
- "In line with rule 192.4, the court must consider whether differences in utility and usability of the form requested are significant enough in the context of the particular case—to override any enhanced burden, cost, or convenience. If the burden or cost is unreasonable compared to the countervailing factors, the trial court may order production in (1) the form the responding party proffers, (2) another form that is proportionally appropriate, or (3) the form requested if (i) there is a particularized need for otherwise unreasonable production efforts and (ii) the court orders the requesting party to 'pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information."¹⁴⁴
- But "[t]he option to shift costs to the requesting party does not, in and of itself, sanctify an order for an unreasonable form of production, because the burdens of delay and expense are not borne only unto the parties, but also the judicial system."¹⁴⁵

The Texas Supreme Court then explained that "[w]hen a reasonably usable form is readily available in the ordinary course of business, the trial court must assess

^{141.} In re Methodist Primary Care Group, 553 S.W.3d 709, 717 (Tex. App.—Houston (14 Dist.), 2018, orig. proceeding) (quoting In re Weekley Homes, L.P., 295 S.W.3d 309, 315, 316 (Tex. 2009)).

^{142.} In re State Farm Lloyds, 520 S.W.3d at 607.

^{143.} In re State Farm Lloyds, 520 S.W.3d at 607 (footnote omitted).

^{144.} In re State Farm Lloyds, 520 S.W.3d at 607 (footnote omitted).

^{145.} In re State Farm Lloyds, 520 S.W.3d at 607 n.39.

§ 13.3

whether any enhanced burden or expense associated with a requested form is justified when weighed against the proportional needs of the case," and "[t]he proportionality inquiry requires case-by-case balancing in light of the following factors:

- 1. Likely benefit of the requested discovery ...
- 2. The needs of the case . . .
- 3. The amount in controversy . . .
- 4. The parties' resources . . .
- 5. Importance of the issues at stake in the litigation ...
- 6. The importance of the proposed discovery in resolving the litigation
- 7. Any other articulable factor bearing on proportionality"¹⁴⁶

As to the first factor, the Supreme Court explained that "[i]f the benefits of the requested form are negligible, nonexistent, or merely speculative, any enhanced efforts or expense attending the requested form of production is undue and sufficient to deny the requested discovery"; "[i]n such cases, quantifying or estimating time and expenses would not be critical, as it may be when benefits clearly exist"; "[a]t the opposite end of the spectrum, a particularized need for the proposed discovery will weigh heavily in favor of allowing discovery as requested but, depending on the force of other prudential concerns, may warrant cost shifting for any 'extraordinary steps' required"; and "[c]ourts should consider cumulative effects rather than viewing benefits and burdens in a vacuum."¹⁴⁷

As to the third factor, the Supreme Court explained that "[a]ccessibility—or relative inaccessibility—of electronic data contributes to increased costs and burdens associated with electronic discovery" and that "the amount in controversy plays a pivotal role in determining whether production in a specified form is justified given the burden or expense required to meet the demand."¹⁴⁸

As to the fourth factor, the Supreme Court explained:

Whether the producing party has the means to fairly and realistically produce in the requested format is a significant proportionality consideration.

^{146.} In re State Farm Lloyds, 520 S.W.3d at 607-11.

^{147.} In re State Farm Lloyds, 520 S.W.3d at 608.

^{148.} In re State Farm Lloyds, 520 S.W.3d at 610.

An expense that is a drop in the bucket to one party, may be insurmountable to another. While this factor is important to the balancing inquiry "considerations of the parties' resources does not foreclose discovery requests addressed to an impecunious party, nor justify unlimited discovery requests addressed to a wealthy party." Rather, "the court must apply the standards in an evenhanded manner that will prevent use of discovery to wage a war of attrition or as a device to coerce a party, whether financially weak or affluent.""

But beyond financial resources, one must also consider whether the requesting party has the technological resources to make proper use of ESI in the form requested. A high-powered luxury sports car is useless to someone who lacks a license to drive it.¹⁴⁹

And, as to the sixth factor, the Supreme Court explained that "[d]iscovery must bear at least a reasonable expectation of obtaining information that will aid the dispute's resolution" and that "[r]easonable discovery does not countenance a 'fishing expedition."¹⁵⁰ As a Texas Court of Appeals decision later explained, the Texas Rules' broad grant of discovery "is limited by the legitimate interests of the opposing party to avoid overly broad requests, harassment, or disclosure of privileged information in keeping with the understanding that discovery is a means to an end, rather than an end in itself."¹⁵¹

The Texas Supreme Court further explained in *In re State Farm Lloyds* that "[d]iscovery is necessarily a collaborative enterprise, and particularly so with regard to electronic discovery" and that "[t]he opposing party must object and support proportionality complaints with evidence if the parties cannot resolve a discovery dispute without court intervention, but the party seeking discovery must comply with proportionality limits on discovery requests and 'may well need to . . . make its own showing of many or all of the proportionality factors."¹⁵²

But, as a threshold matter, "rule 196.4 requires specificity," and "[t]he purpose of rule 196.4's specificity requirement is to ensure that requests for electronic information are clearly understood and disputes avoided."¹⁵³

^{149.} In re State Farm Lloyds, 520 S.W.3d at 610-11 (footnotes omitted).

^{150.} In re State Farm Lloyds, 520 S.W.3d at 610-11 (footnotes omitted).

^{151.} In re Toyota Motor Sales, U.S.A., Inc., No. 05-18-00734-CV, 2018 WL 3484280, at *2 (Tex. App.—Dallas, July 19, 2018, orig. proceeding).

^{152.} In re State Farm Lloyds, 520 S.W.3d at 614 (footnotes omitted; quoting Carr v. State Farm Mut. Auto. Ins. Co., 312 F.R.D. 459, 468–69 (N.D. Tex. 2015)).

Responding to Discovery Requests and Discovery Disputes

For example, the Texas Supreme Court in *In re Weekley Homes, L.P.* explained that a rule 196.4 request failed the specificity requirement because it did not expressly seek deleted e-mail but that "even though it was not stated in [the party's] written request that deleted e-mails were included within its scope, that [the requesting party] thought they were and was seeking this form of electronic information became abundantly clear in the course of discovery and before the hearing on the motion to compel."¹⁵⁴ "Because the scope of discovery sought 'was understood before trial court intervention, [the producing party] was not prejudiced by [the requesting party's] failure to follow the rule."¹⁵⁵

"Rule 196.4 is clear that when a specific request for electronic data has been made, the responding party is required to produce responsive electronic data that is reasonably available in the ordinary course cf business."¹⁵⁶ But "[o]nce a specific request is made the parties can, and should, communicate as to the particularities of a party's computer storage system and potential methods of retrieval to assess the feasibility of their recovery."¹⁵⁷

The Supreme Court in In re Weekley Homes explained in summary:

A fundamental tenet of our discovery rules is cooperation between parties and their counsel, and the expectation that agreements will be made as reasonably necessary for efficient disposition of the case. Tex. R. Civ. P. 191.2. Accordingly, prior to promulgating requests for electronic information, parties and their attorneys should share relevant information concerning electronic systems and storage methodologies so that agreements regarding protocols may be reached or, if not, trial courts have the information necessary to craft discovery orders that are not unduly intrusive or overly burdensome.

With these overriding principles in mind, we summarize the proper procedure under rule 196.4:

. . . .

^{153.} In re Weekley Homes, L.P., 295 S.W.3d 309, 314 (Tex. 2009); see also In re Shipman, 540 S.W.3d 562, 566–67 (Tex. 2018).

^{154.} In re Weekley Homes, L.P., 295 S.W.3d at 314.

^{155.} In re Shipman, 540 S.W.3d at 566 (quoting In re Weekley Homes, L.P., 295 S.W.3d at 314-15).

^{156.} In re Methodist Primary Care Group, 553 S.W.3d 709, 717 (Tex. App.—Houston [14th Dist.], 2018, orig. proceeding).

^{157.} In re Weekley Homes, L.P., 295 S.W.31 at 314 (footnote omitted).

- The party seeking to discover electronic information must make a specific request for that information and specify the form of production. Tex. R. Civ. P. 196.4.
- The responding party must then produce any electronic information that is "responsive to the request and . . . reasonably available to the responding party in its ordinary course of business."
- If "the responding party cannot—through reasonable efforts retrieve the data or information requested or produce it in the form requested," the responding party must object on those grounds.
- The parties should make reasonable efforts to resolve the dispute without court intervention. Tex. R. Civ. P. 191.2.
- If the parties are unable to resolve the dispute, either party may request a hearing on the objection, Tex. R. Civ. P. 193.4(a), at which the responding party must demonstrate that the requested information is not reasonably available because of undue burden or cost, Tex. R. Civ. P. 193.4(b).
- If the trial court determines the requested information is not reasonably available, the court may nevertheless order production upon a showing by the requesting party that the benefits of production outweigh the burdens imposed, again subject to rule 192.4's discovery limitations.
- If the benefits are shown to outweigh the burdens of production and the trial court orders production of information that is not reasonably available, sensitive information should be protected and the least intrusive means should be employed. Tex. R. Civ. P. 192.6(b). The requesting party must also pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information. Tex. R. Civ. P. 196.4.
- Finally, when determining the means by which the sources should be searched and information produced, direct access to another party's electronic storage devices is discouraged, and courts should be extremely cautious to guard against undue intrusion.¹⁵⁸

^{158.} In re Weekley Homes, L.P., 295 S.W.3d at 321-22.

Responding to Discovery Requests and Discovery Disputes

Finally, the Texas Supreme Court explained in *In re State Farm Lloyds* that "[m]eeting and conferring to resolve e-discovery disputes without court intervention is essential because discovery of electronic data involves case-specific considerations and each side possesses unique access to information concerning reasonable and viable production methods, resources (technological or monetary, for instance), and needs."¹⁵⁹

§ 13.3:2 General Requirements for Discovery Requests

But Texas state court requests for ESI and responses to them still depend on, and are governed by, many of the general rules for discovery requests and responses. As with the federal rules, properly responding or objecting to a rule 196.4 request requires an attorney to understand and consider the Texas rules' limitations on a request's scope and form.

"Texas Rule of Civil Procedure 192.3 addresses the scope of discovery in Texas."¹⁶⁰ Under Texas Rule of Civil Procedure 192.3, "[i]n general, a party may obtain discovery regarding any matter that is not privileged and is relevant to the subject matter of the pending action, whether it relates to the claim or defense of the party seeking discovery or the claim or defense of any other party," and "[i]t is not a ground for objection that the information sought will be inadmissible at trial if the information sought appears reasonably calculated to lead to the discovery of admissible evidence."¹⁶¹ The Texas Supreme Court "broadly construe[s] the phrase 'relevant to the subject matter' to provide litigants the opportunity 'to obtain the fullest knowledge of the facts and issues prior to trial," where "[e]vidence is relevant if '(a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the act on."¹⁶²

"These liberal bounds, however, have limits, and 'discovery requests must not be overbroad."¹⁶³ "A request is not 'overbroad merely because [it] may call for some information of doubtful relevance' so long as it is 'reasonably tailored to include only

163. In re National Lloyds Insurance Company, 507 S.W.3d 219, 223 (Tex. 2016) (orig. proceeding) (per curiam) (footnotes omitted).

^{159. 520} S.W.3d at 606.

^{160.} In re City of Dickinson, 568 S.W.3d 642, 646 (Tex. 2019).

^{161.} Tex. R. Civ. P. 192.3(a).

^{162.} In re National Lloyds Insurance Company, 532 S.W.3d 794, 808 (Tex. 2017) (orig. proceeding) (footnotes omitted; quoting Ford Motor Co. v. Castillo, 279 S.W.3d 656, 664 (Tex. 2009); Tex. R. Evid. 401).

matters relevant to the case.¹¹⁶⁴ "A central consideration in determining overbreadth is whether the request could have been more narrowly tailored to avoid including tenuous information and still obtain the necessary, pertinent information.¹⁶⁵ The Texas Supreme Court has explained that "[r]easonable' discovery necessarily requires some sense of proportion" and that, "[w]ith today's technology, it is the work of a moment to reissue every discovery request one has ever sent to [a similar defendant] before" but that "by definition such a request is not 'reasonably tailored.¹¹⁶⁶

But "whether a request for discovery is overbroad is distinct from whether it is burdensome or harassing," and "[o]verbroad requests for irrelevant information are improper whether they are burdensome or not."¹⁶⁷

But the responding party must support "complaints of burdensomeness and harassment with . . . more than general allegations. Without some more detailed explanation and proof, [an objecting party will not meet] the basic requirements for limiting the scope of discovery under the rules of civil procedure."¹⁶⁸

And Texas Rule of Civil Procedure 191.3 largely tracks Federal Rule of Civil Procedure 26(g):

Signing of Disclosures, Discovery Requests, Notices, Responses, and Objections

- (a) Signature required. Every disclosure, discovery request, notice, response, and objection must be signed:
 - (1) by an attorney, if the party is represented by an attorney, and must show the attorney' State Bar of Texas identification number, address, telephone number, and fax number, if any; or
 - (2) by the party, if the party is not represented by an attorney, and must show the party's address, telephone number, and fax number, if any.

^{164.} In re National Lloyds Insurance Company, 449 S.W.3d 486, 488 (Tex. 2014) (orig. proceeding) (footnote omitted).

^{165.} In re CSX Corp., 124 S.W.3d 149, 153 (Tex. 2003).

^{166.} In re Allstate County Mut. Ins. Co., 227 S.W.3d 667, 670 (Tex. 2007).

^{167.} In re National Lloyds Insurance Company, 449 S.W.3d 486, 488 (Tex. 2014) (orig. proceeding) (footnote omitted).

^{168.} In re Alford Chevrolet-Geo, 997 S.W.2d 173, 184 (Tex. 1999) (citing Tex. R. Civ. P. 192.4, 192.6).

- (b) Effect of signature on disclosure. The signature of an attorney or party on a disclosure constitutes a certification that to the best of the signer's knowledge, information, and belief, formed after a reasonable inquiry, the disclosure is complete and correct as of the time it is made.
- (c) Effect of signature on discovery request, notice, response, or objection. The signature of an attorney or party on a discovery request, notice, response, or objection constitutes a certification that to the best of the signer's knowledge, information, and belief, formed after a reasonable inquiry, the request, notice, response, or objection:
 - is consistent with the rules of civil procedure and these discovery rules and warranted by existing law or a good faith argument for the extension, modification, or reversal of existing law;
 - (2) has a good faith factual basis;
 - (3) is not interposed for any improper purpose, such as to harass or to cause unnecessary delay or needless increase in the cost of litigation; and
 - (4) is not unreasonable or unduly burdensome or expensive, given the needs of the case, the discovery already had in the case, the amount in controversy, and the importance of the issues at stake in the litigation.
- (d) Effect of failure to sign. If a request, notice, response, or objection is not signed, it must be stricken unless it is signed promptly after the omission is called to the attention of the party making the request, notice, response, or objection. A party is not required to take any action with respect to a request or notice that is not signed.
- (e) Sanctions. If the certification is false without substantial justification, the court may, upon motion or its own initiative, impose on the person who made the certification, or the party on whose behalf the request, notice, response, or objection was made, or both, an appropriate sanction as for a frivelous pleading or motion under Chapter 10 of the Civil Practice and Remedies Code.¹⁶⁹

169. Tex. R. Civ. P. 191.3.

§ 13.3:3 General Requirements for Responses and Objections

The Texas rules also specifically address how to respond to a discovery request:

A party must respond to written discovery in writing within the time provided by court order or these rules. When responding to written discovery, a party must make a complete response, based on all information reasonably available to the responding party or its attorney at the time the response is made. The responding party's answers, objections, and other responses must be preceded by the request to which they apply.¹⁷⁰

And Texas Rule of Civil Procedure 193.2 governs objections:

- (a) Form and time for objections. A party must make any objection to written discovery in writing—either in the response or in a separate document—within the time for response. The party must state specifically the legal or factual basis for the objection and the extent to which the party is refusing to comply with the request.
- (b) Duty to respond when partially objecting; objection to time or place of production. A party must comply with as much of the request to which the party has made no objection unless it is unreasonable under the circumstances to do so before obtaining a ruling on the objection. If the responding party objects to the requested time or place of production, the responding party must state a reasonable time and place for complying with the request and must comply at that time and place without further request or order.
- (c) Good faith basis for objection. A party may object to written discovery only if a good faith factual and legal basis for the objection exists at the time the objection is made.
- (d) Amendment. An objection or response to written discovery may be amended or supplemented to state an objection or basis that, at the time the objection or response initially was made, either was inapplicable or was unknown after reasonable inquiry.
- (e) Waiver of objection. An objection that is not made within the time required, or that is obscured by numerous unfounded objections, is waived unless the court excuses the waiver or good cause shown.¹⁷¹

^{170.} Tex. R. Civ. P. 193.1.

Texas Rule of Civil Procedure 193.3 specifically addresses how to assert a privilege, which includes work product protection.¹⁷² Under Texas Rule of Civil Procedure 193.2(f), "[a] party should not object to a request for written discovery on the grounds that it calls for production of material or information that is privileged but should instead comply with rule 193.3," and "[a] party who objects to production of privileged material or information does not waive the privilege but must comply with rule 193.3 when the error is pointed out."¹⁷³ And, under Texas Rule of Civil Procedure 193.4, "[a]ny party may at any reasonable time request a hearing on an objection or claim of privilege must present any evidence necessary to support the objection or privilege."¹⁷⁴

Texas Rule of Civil Procedure 196.6 provides that, "[u]nless otherwise ordered by the court for good cause, the expense of producing items will be borne by the responding party and the expense of inspecting, sampling, testing, photographing, and copying items produced will be borne by the requesting party."¹⁷⁵

Under Texas Rule of Civil Procedure 192.6-

[A] person from whom discovery is sought, and any other person affected by the discovery request, may move within the time permitted for response to the discovery request for an order protecting that person from the discovery sought. A person should not move for protection when an objection to written discovery or an assertion of privilege is appropriate, but a motion does not waive the objection or assertion of privilege. If a person seeks protection regarding the time or place of discovery, the person must state a reasonable time and place for discovery with which the person will comply.¹⁷⁶

These rules "explicitly encourage trial courts to limit discovery when 'the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the impor-

- 173. Tex. R. Civ. P. 193.2(f).
- 174. Tex. R. Civ. P. 193.4.
- 175. Tex. R. Civ. P. 196.6.
- 176. Tex. R. Civ. P. 192.6.

^{171.} Tex. R. Civ. P. 193.2(a)-(e).

^{172.} Tex. R. Civ. P. 193.3, 192.5.

tance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.¹⁷⁷

But "[a] party resisting discovery, however, cannot simply make conclusory allegations that the requested discovery is unduly burdensome or unnecessarily harassing. The party must produce some evidence supporting its request for a protective order."¹⁷⁸

And, even when a motion for protection is filed, "[a] person must comply with a request to the extent protection is not sought unless it is unreasonable under the circumstances to do so before obtaining a ruling on the motion."¹⁷⁹

^{177.} In re Alford Chevrolet-Geo, 997 S.W.2d 173, 181 (Tex. 1999) (quoting Tex. R. Civ. P. 192.4(b)).

^{178.} In re Alford Chevrolet-Geo, 997 S.W.2d at 181.

^{179.} Tex. R. Civ. P. 192.6.

Chapter 14

Cost Shifting and 28 U.S.C. § 1920

Julia W. Mann and Judge Xavier Rodriguez

§ 14.1 Introduction

"Broad discovery is an important tool for the litigant"¹ Most litigators, however, would agree that the economic pressures related to discovery, particularly electronic discovery, are one of the biggest issues in modern-day litigation. E-discovery has evolved into an expensive endeavor, spawning a cottage industry of products, technology, and vendors to search, collect, and produce electronically stored information (ESI).² From in-house servers to flash drives to cloud computing and a multitude of personal electronic devices, there is an astounding amount of storage repositories available on which to conduct discovery. In addition to computers and backup tapes, relevant information is now stored on smart phones, tablets, laptops, blogs, and social media.³ Needless to say, searching through all the potential forms of ESI for relevant discoverable information is often an expensive task that can be burdensome for both the litigant and the client.

Both the Federal Rules of Civil Procedure and the Texas Rules of Civil Procedure provide mechanisms in the discovery phase that may yield opportunities for parties to shift discovery costs.⁴ This chapter explores such mechanisms and provides illustrations from recent cases regarding how courts have treated the rules. Case law regarding how a court may exercise cost-shifting authority is generally unsettled in the context of e-discovery. However, as discussed more fully in this chapter, the trend is to allow cost shifting and cost sharing to protect from "undue burden or expense."⁵

5. See, e.g., Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999).

^{1.} WWP, Inc. v. Wounded Warriors Family Support, Inc., 628 F.3d 1032, 1039 (8th Cir. 2011).

^{2.} See Nishad Shevde, How E-Discovery Trends are Re-Shaping E-Discovery Teams, Law.com (July 23, 2019), www.law.com/2019/07/23/how-e-discovery-trends-are-reshaping-e-discovery-teams; see also Zachary G. Newman, Hot Topics and Recent Court Decisions in E-Discovery, American Bar Association (June 20, 2012), www.americanbar.org/groups/litigation/committees/corporate-counsel/articles/2012/spring2012-hot-topics-and-recent-court-decisions-in-e-discovery/.

^{3.} See VOOM HD Holdings, LLC v. EckoStar Satellite L.L.C., 939 N.Y.S.2d 321 (N.Y. App. Div. 2012).

^{4.} See Fed. R. Civ. P. 26(b)(2); see also Tex. R. Civ. P. 194.6.

Section 14.2 of this chapter explores the evolution of the Federal Rules of Civil Procedure for cost shifting and consideration of proportionality. Section 14.3 discusses various costs that may be recovered by a prevailing party in federal court pursuant to Fed. R. Civ. P. 54(d) and 28 U.S.C. § 1920. Section 14.4 explores the Texas rule regarding cost shifting and cost sharing.

§ 14.2 Evolution of Federal Rule of Civil Procedure 26

§ 14.2:1 American Rule Presumptively Prohibits Cost Shifting or Cost Sharing

The historic presumption in the United States is that each party bears its own litigation costs in the absence of statutory authorization or a contractual agreement providing otherwise.⁶ As such, the "American Rule" prohibits the shifting of attorney's fees in most cases.⁷ The party seeking cost shifting or cost sharing bears the burden of overcoming that presumption.⁸ In recent years, modifications have been made to the Federal Rules of Civil Procedure that open the door to not only limiting discovery on electronically stored information, but to providing specific conditions that may shift the cost of accessing and providing electronic data.

§ 14.2:2 Fed. R. Civ. P. 26 Gives Court Discretion to Order Cost Shifting or Cost Sharing

The impact of ESI on the issue of cost shifting and the consideration of proportionality is evident from the civil discovery rules themselves. Fed. R. Civ. P. 26 governs the scope and limits on discovery. Before the 2015 amendment, rule 26 did not expressly impose a proportionality limit on discovery. With the expansion of ESI available to parties from a variety of sources, many of which can be duplicative, the 2015 amendment sought to acknowledge the potentially overwhelming costs and provide a means for limiting overreaching e-discovery. Rule 26(b)(1) provides that the discovery must be limited based on the requirements of the case as follows: "Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or

^{6.} See Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978); see also Alyeska Pipeline Service Co. v. Widerness Society, 421 U.S. 240, 247 (1975).

^{7.} Chambers v. NASCO, Inc., 501 U.S. 32, 33 (1991).

^{8.} Last Atlantis Capital, LLC v. AGS Specialist Partners, No. 04 C 0397, 2011 WL 6097769, at *2 (N.D. III. Dec. 5, 2011) (citing The Sedona Conference, Sedona Conference Commentary on Non-Party Production & Rule 45 Subpoenas, 9 Sedona Conf. J. 197, 201 (2008)).

defense *and proportional to the needs of the case*" Rule 26(b)(1) sets forth six factors that courts should weigh in making a proportionality ruling, as follows:

- important of the issues at stake in the action;
- the amount in controversy;
- the parties' relative access to relevant information;
- the parties' resources;
- the importance of the discovery in resolving the issues; and
- whether the burden or expense of the proposed discovery outweighs its likely benefit.

Fed. R. Civ. P. 26(b)(1) (emphasis added); *see also Fed. Trade Comm'n v. Liberty Supply Co.*, No. 4:15-CV-829, 2016 WL 4272706, at *4 (E.D. Tex. Aug. 15, 2016) (the party resisting discovery bears the burden to clarify and explain its objections and to provide support for those objections).

In Oxbow Carbon & Minerals, LLC v Union Pac. R.R.,⁹ the Court analyzed each of these factors finding that the requests were "neither unduly burdensome nor unreasonably expensive in light of the facts of the case" and that "the instant circumstances do not warrant shifting costs." Oxbow claimed it paid the defendants more than \$50 million in illegal fuel surcharges as a result of an antitrust conspiracy. Defendants requested that the Court compel Oxbow to add William I. Koch ("Koch"), Oxbow's founder, CEO, and principal owner as a document custodian whose records would be searched for material responsive to Plaintiffs' discovery requests. Defendants argued that Koch's records contained information that would reveal that market forces—as opposed to Defendants' alleged collusion—contributed to the increasing rail freight costs and any of Oxbow's lost profits. Defendants asserted, and the Court agreed, that their discovery request was proportionate and reasonable in light of the facts of this case, including the tens of millions of dollars that Oxbow sought in damages.

Fed. R. Civ. P. 26(b)(2) allows courts to place specific limits on electronically stored information.¹⁰ Under rule 26(b)(2)(B), a responding party need not produce ESI from sources that it identifies as not reasonably accessible because of undue burden or cost.¹¹ If the requesting party moves to compel discovery of such information, the responding party must show that the information is not reasonably accessible because

^{9. 322} F.R.D. 1 (D.D.C. Sept. 11, 2017).

^{10.} Fed. R. Civ. P. 26(b)(2)(B).

of undue burden or cost.¹² Once that showing is made, a court may order discovery only for good cause, subject to the provisions of rule 26(b)(2)(C).¹³

Further, the rule expressly provides that "the court may specify conditions for the discovery," again providing discretion for each individual case.¹⁴ The court's cost-benefit analysis under rule 26(b)(2)(C) regarding weighing the burden or expense of the proposed discovery against its benefit has become known as the "proportionality rule."¹⁵ In assessing whether to limit discovery, one of the factors a court considers is whether "the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive."¹⁶

It is important to note that the responding party has the burden of proof on a motion for cost shifting, and the cost that is shifted is only the cost of retrieving the data, not the cost of reviewing that data before production. If a party elects to conduct a pageby-page data review, it will singly bear that cost. The cost of harvesting or securing the data is the cost that may be shared or shifted. In *Estate of Shaw v. Marcus*,¹⁷ the court ordered the plaintiff to pay for seventy percent of forensic examination costs (primarily due to discovery misconduct). But the court noted that as "a general rule, where cost shifting is appropriate, only the costs of restoration and searching should be shifted. Thus, Plaintiff's seventy-percent share only includes costs for restoration and searching, and not, as the Shaw Family requests, any expenses incurred in the course of review."

14. The discretion to specify conditions is expressly provided to the court in the last sentence of Fed. R. Civ. P. 26(b)(2)(B).

15. Fed. R. Civ. P. 26(b)(2)(C); see also Robert K. Dixon, What's Proportionality Got to Do with It? An Update on the Revised Federal Discovery Rules, American Bar Association (May 15, 2017), www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/articles/2017/whats -proportionality-got-to-do-with-it/.

16. Fed. R. Civ. P. 26(b)(2)(C)(i).

17. No. 14CIV3849NSRJCM, 2017 WL 825317, at *6 (S.D.N.Y. Mar. 1, 2017).

^{11.} Fed. R. Civ. P. 26(b)(2)(B) ("A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.").

^{12.} Fed. R. Civ. P. 26(b)(2)(B) ("On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost.").

^{13.} Fed. R. Civ. P. 26(b)(2)(B) ("If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of rule 26(b)(2)(C).").

Finally, although there is a presumption that the responding party must bear the expense of complying with discovery requests,¹⁸ a court has further discretion under Federal Rule of Civil Procedure 26(c) to cost shift or to condition discovery on the requesting party's payment of the costs of the discovery.¹⁹ Pursuant to Fed. R. Civ. P. 26(c), a district court may issue an order protecting the responding party from undue burden or expense by allocating expenses for the disclosure or discovery.²⁰ Such an order may be granted only on the motion of the responding party and "for good cause shown." Fed. R. Civ. P. 26(c).

§ 14.2:3 Zubulake Trend Allows Cost Shifting When Inaccessibility Is a Factor

Cost shifting entered the world of e-discovery with the *Zubulake* decisions in the context of production of ESI from "inaccessible" sources.²¹ In *Zubulake*, the court stated that "cost shifting should be considered only when electronic discovery imposes an 'undue burden or expense' on the responding party."²² According to the court, "whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format (a distinction that corresponds closely to the expense of production)."²³ The court concluded that whether electronic data is accessible or inaccessible depends largely on the media on which it is stored.²⁴ Information deemed "accessible" is stored in a readily usable format.²⁵

19. Fed. R. Civ. P. 26(c); see also Foreclosure Management Co. v. Asset Management Holdings, LLC, No. 07-2388-DJW, 2008 WL 3822773, at *7 (D. Kan. Aug. 13, 2008).

20. Fed. R. Civ. P. 26(c)(1)(B).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003). The decisions include Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003) (Zubulake I); Zubulake v. UBS Warburg LLC, 230 F.R.D. 290 (S.D.N.Y. 2003) (Zubulake II); Zubulake v. UBS Warburg LLC, 216 F.R.D. 280 (S.D.N.Y. 2003) (Zubulake III); Zubulake v. UBS Warburg LLC, 220 F.R.D. 212 (S.D.N.Y. 2003) (Zubulake IV); Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004) (Zubulake V).

22. Zubulake I, 217 F.R.D. at 318. The Zubulake factors include (1) the degree to which the request for information is designed to discover germane information, (2) the availability of the same information from different sources, (3) the cost of production as compared to the amount in controversy, (4) the cost of production as compared to the resources of each party, (5) the parties' relative abilities to control discovery costs and their incentives to control costs, (6) the degree of importance of the issues being decided in the litigation, and (7) the relative benefits to each of the parties in obtaining the information at issue.

§ 14.2

^{18.} See, e.g., Hawa v. Coatesville Area Sch. Dist., No. CV 15-4828, 2017 WL 1021026, at *1 (E.D. Pa. Mar. 16, 2017) (denying cost-shifting motion); Oxbow Carbon & Minerals LLC v. Union Pac. R.R. Co., 322 F.R.D. 1, 11 (D.D.C. 2017) ("Defendants' proposed discovery does not impose an undue burden or expense that warrants a reallocation of expenses.").

^{23.} Zubulake I, 217 F.R.D. at 318.

^{24.} Zubulake I, 217 F.R.D. at 318.

^{25.} Zubulake I, 217 F.R.D. at 320.

"Inaccessible data" must be restored or reconstructed before the data is usable.²⁶ The *Zubulake* court then went on to identify "active, online data," "near-line data," and "offline storage" as accessible formats and "backup tapes" and "erased, fragmented, or damaged data" as inaccessible formats.²⁷ In *Zubulake*, much of the data was contained in e-mails stored on backup tapes.²⁸ In order to search the tapes for responsive e-mails, the tapes would have to be reconstructed to make the data usable.²⁹ As such, the court concluded that considering cost shifting was appropriate.³⁰

Post-Zubulake, some courts conclude that "cost shifting does not even become a possibility unless there is first a showing of inaccessibility."³¹ For example, in *W* Holding *Co., Inc. v. Chartis Insurance Co. of Puerto Rico*, the court noted that "[w]hile cost and burden are critical elements in determining accessibility, a showing of undue burden is not sufficient by itself to trigger a finding of inaccessibility."³² The court stated "sheer volume of data may make its production expensive, but that alone does not bring it within the scope of rule 26(b)(2)(B). Rather, the cost or burden must be associated with some technological feature that inhibits accessibility."³³ The court concluded that because the responding party did not show that access to the data was hindered by any unique technological hurdles, it failed to trigger rule 26(b)(2)(B) and was therefore not entitled to categorically label the ESI as "not reasonably accessible."³⁴

- 26. Zubulake I, 217 F.R.D. at 320.
- 27. Zubulake I, 217 F.R.D. at 318-19.
- 28. Zubulake I, 217 F.R.D. at 320.
- 29. Zubulake I, 217 F.R.D. at 320.
- 30. Zubulake I, 217 F.R.D. at 320.

31. See, e.g., Peskoff v. Faber, 240 F.R.D. 26, 31 (D.D.C. 2007) ("[A]ccessible data must be produced at the cost of the producing party; cost shifting does not even become a possibility unless there is first a showing of inaccessibility."); *Pipefitters Local No. 636 Pension Fund v. Mercer Human Resource Consulting, Inc.*, No. 05-CV-74326, 2007 WL 2080365, at *2 (E.D. Mich. July 19, 2007).

32. W Holding Co., Inc. v. Chartis Insurance Co. of Puerto Rico, 293 F.R.D. 68, 72 (D.P.R. 2013) (quoting Chen-Oster v. Goldman, Sachs & Co., 285 F.R.D. 294, 301 (S.D.N.Y. 2012)).

33. W Holding Co., 293 F.R.D. at 72–73 (quoting Chen-Oster, 285 F.R.D. at 301); see also Juster Acquisition Co., LLC v. North Hudson Sewerage Authority, No. 12-3427 (JLL), 2013 WL 541972, at *4 (D.N.J. Feb. 11, 2013) ("Here, NHSA, as the responding party, has failed to satisfy its burden of showing that the ESI sought by Juster is inaccessible. NHSA has not asserted that any of the requested data is located on backup tapes. It has not asserted that any of the requested data is erased, fragmented, or damaged in any way. To the contrary, by asserting that it has hired an outside vendor to perform the word searches, NHSA has acknowledged that the ESI is accessible. It has also failed to show that the ESI sought by Juster imposes an 'undue' burden or expense. Rather, the Court finds that NHSA seeks merely to avoid the cost associated with what it presumes to be duplicative and expensive word searches. As a result, the Court cannot find that the ESI requested by Juster falls into either category of 'inaccessible' electronic data. Because such data is in fact accessible to NHSA, defendant must bear the attendant discovery costs.") (citations omitted).

Other courts also continue to focus on inaccessibility as a prerequisite for cost shifting.³⁵ In Nogle v. Beech Street Corp., the plaintiff requested that the defendant be required to restore and search archived e-mails stored on backup tapes.³⁶ The plaintiff argued that the defendant should be ordered to bear the costs of restoring and searching the requested ESI as a sanction for the defendant's failing to produce documents after the plaintiff filed a motion to compel.³⁷ The court noted that shifting the cost of production to the requesting party should be applied only when the requested information is not reasonably accessible and the responding party has not caused the information to become inaccessible after it was on notice that the information was relevant to pending or reasonably anticipated litigation.³⁸ The court cited to Zubulake to assert that information stored on archival backup tapes is generally considered not reasonably accessible.³⁹ In Nogle, however, the court never reached the cost-shifting decision because it had not been provided with a reasonable estimate by a qualified vendor regarding the cost for restoring the ESI or other expenses that may be incurred in searching the ESI once it was restored.⁴⁰ As such, the court was not in a position to determine whether all or a portion of that expense should be shifted to the plaintiff.

In *Kleen Products LLC v. Packaging Corp. of America*, the court noted that other courts generally agree that backup tapes are presumptively inaccessible.⁴¹ In addition, the defendants demonstrated a cost burden to restoring the backup media.⁴² The defendants provided affidavits indicating that to restore the backup tapes would cost

- 35. Nogle v. Beech Street Corp., No. 10 C 5711, 2012 WL 3687570, at *8 (D. Nev. Aug. 27, 2012).
- 36. Nogle, 2012 WL 3687570, at *6.
- 37. Nogle, 2012 WL 3687570, at *6.
- 38. Nogle, 2012 WL 3687570, at *8.
- 39. Nogle, 2012 WL 3687570, at *8.
- 40. Nogle, 2012 WL 3687570, at *8.

41. No. 10-C-5711, 2012 WL 4498465, at *18 (N.D. III. Sept. 28, 2012); see, e.g., Zubulake I, 217 F.R.D. at 319–20 ("Inaccessible' data . . . is not readily usable. Backup tapes must be restored using a process similar to that previously described, fragmented data must be defragmented, and erased data must be reconstructed, all before the data is usable. That makes such data inaccessible."); see also Major Tours, Inc. v. Colorel, No. 05-3091(JBS/JS), 2009 WL 3446761, at *3 (D.N.J. Oct. 20, 2009) (noting that backup tapes are "typically classified as inaccessible"); Go v. Rockefeller University, 280 F.R.D. 165, 175–76 (S.D.N.Y. 2012) ("Information stored on backup tapes is generally considered 'not reasonably accessible."); Clean Harbors Environmental Services, Inc. v. ESIS, Inc., No. 09 C 3789, 2011 WL 1897213, at *2 (N.D. III. May 17, 2011) ("Courts have already agreed that when information is stored on backup tapes, it is 'likened to paper records locked inside a sophisticated safe to which no one has the key or combination.' ESIS has given us no reason to believe that the information on the backup tapes in this case would be more easily accessible.") (quoting Zubulake III, 216 F.R.D. at 291).

42. Kleen Products, 2012 WL 4498465, at *18.

^{34.} W Holding Co., 293 F.R.D. at 73.

each defendant at least \$200,000, with some estimates well over \$1,000,000.⁴³ The court found that the plaintiffs' request to produce the backup tapes was premature.⁴⁴ There was no discovery cutoff date in the case, and the plaintiffs were only twenty percent complete with their first-level review of the defendants' documents.⁴⁵ The court concluded that the plaintiffs should complete their review of the defendants' ESI, including the information produced from the additional custodians, before seeking to have archived backup tapes restored.⁴⁶

§ 14.2:4 Trend Is to Rely Less on Inaccessibility

Fifteen years after *Zubulake* and after two notable amendments to the Federal Rules of Civil Procedure, most recently in 2015, courts are beginning to expand cost shifting to ESI that is not necessarily inaccessible. In *Surplus Source Group, LLC v. Mid America Engine, Inc.*, without addressing accessibility, the court ordered cost shifting for a third ESI search on the basis of the plaintiffs' failure to accurately communicate search terms to the defendants in the prior two ESI searches.⁴⁷ The court noted that as the responding party, the defendants should bear the cost of obtaining their own ESI.⁴⁸ The court went on to explain that prior to conducting the first ESI search, the defendants requested from the plaintiffs the desired search terms that would yield the documents the plaintiffs were seeking.⁴⁹ However, the plaintiffs failed to disclose the desired search terms until after two ESI searches had been conducted.⁵⁰ The court concluded that the cost of searching the ESI for the relevant records exceeded what it would have been had the plaintiffs been more diligent in communicating their search terms to the defendants.⁵¹ As such, the court ordered the plaintiffs to bear the costs of the third ESI search.⁵²

Similarly, in *Adair v. EQT Production Company*, accessibility of the ESI was not the issue before the court; both parties admitted that the ESI was readily accessible and

- 43. Kleen Products, 2012 WL 4498465, at *18.
- 44. Kleen Products, 2012 WL 4498465, at *18.
- 45. Kleen Products, 2012 WL 4498465, at *18.
- 46. Kleen Products, 2012 WL 4498465, at *18.
- 47. No. 4:08-CV-049, 2009 WL 961207, at *2 (E.D. Tex. Apr. 8, 2009).
- 48. Surplus Source Group, 2009 WL 961207, at *2.
- 49. Surplus Source Group, 2009 WL 961207, at *2.
- 50. Surplus Source Group, 2009 WL 961207, at *2.
- 51. Surplus Source Group, 2009 WL 961207, at *2.
- 52. Surplus Source Group, 2009 WL 961207, at *2.

was relevant and material to the issues in the case.⁵³ Rather, the issue was whether the cost of reviewing the ESI should be shifted to the requesting party.⁵⁴ The court noted that "little case law" exists regarding whether the cost of review can be shifted or whether discovery should be limited based solely on the cost of review.⁵⁵ However, the court stated that rule 26(b)(2)(C)(iii) gives the court the ability to limit the frequency or extent of discovery "regardless of accessibility-whenever the burden or expense of the proposed discovery outweighs its likely benefit."⁵⁶ Based on rule 26(b)(2)(C)(iii) and the court's "wide latitude in controlling discovery," the court held the cost of reviewing ESI may be considered in determining whether discovery imposes an undue burden or cost on a responding party and whether to shift costs of such review, either in whole or in part, to the requesting party.⁵⁷

Additionally, in *U.S. ex rel. Carter v. Bridgepoint Educ., Inc.*, the court found so long as "the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues," the cost of even accessible ESI's production may be shifted to a party that has not shown its peculiar relevance to the claims and defenses at hand.⁵⁸

Other courts have held that despite the accessibility of the information being sought, rule 26(c) permits cost shifting as part of enforcing proportionality limits.⁵⁹ In *F.D.I.C. v. Brudnicki*, the FDIC, as receiver for a failed bank, brought a negligence action against eight of the bank's former directors.⁶⁰ The defendants sought production of documents relating to eleven loan transactions at issue and to the allegations in the complaint.⁶¹ When cost shifting was raised, the defendants argued that because the ESI was not inaccessible, the *Zubulake* factors for determining whether there should be cost shifting did not apply.⁶² The *Brudnicki* court found that there were several rea-

- 53. No. 1:10cv00037, 2012 WL 1965880, at *4 (W.D. Va. May 31, 2012).
- 54. Adair, 2012 WL 1965880, at *4.
- 55. Adair, 2012 WL 1965880, at *4.
- 56. Adair, 2012 WL 1965880, at *4 (citing Fed. R. Civ. P. 26(b)(2)(C)(iii)).

57. Adair, 2012 WL 1965880, at *4 (noting that "the court may consider the cost of review of ESI for privileged or responsive information in deciding whether discovery imposes an undue burden or cost on a responding party . . . if the court were inc ined to limit discovery based on the burden or cost of the review . . . the court could shift the costs of that review, either in whole or in part, to the requesting party").

- 58. U.S. ex rel. Carter v. Bridgepoint Educ., Inc., 305 F.R.D. 225, 240 (S.D. Cal. 2015).
- 59. F.D.I.C. v. Brudnicki, 291 F.R.D. 669, 676 (N.D. Fla. 2013).
- 60. Brudnicki, 291 F.R.D. at 671-72.
- 61. Brudnicki, 291 F.R.D. at 674.

sons that justified the defendants paying some of the cost of producing the ESI, even assuming the document management system database did not fall within the definition of inaccessible ESI.⁶³ First, the FDIC had already incurred more than \$624,000 in costs for collection, processing, and uploading of the files and documents of the bank into the DMS database.⁶⁴ The defendants would be required to pay only a \$.06 per page charge for converting a document to a TIFF format and a nominal charge for uploading the data to the relativity database.⁶⁵ Second, the court noted that rule 26(b)(2)(C) provides authority for shifting costs as part of the enforcement of proportionality limits.⁶⁶ Among the factors the court may consider when enforcing proportionality limits are (1) the specificity of the discovery requests, (2) the likelihood of discovering critical information, (3) the purposes for which the responding party maintains the requested data, (4) the relative benefit to the parties of obtaining the information, (5) the total cost associated with the production, (6) the relative ability of each party to control costs and its incentive to do so, and (7) the resources available to each party.⁶⁷

In *Costantino v. City of Atlantic City*, the plaintiff sought the production of internal affairs files in connection with an assault case involving two police officers. Although the plaintiff was willing to limit her request to a "representative sample," the ensuing debate over the scope of a representative sample resulted in an order that all two thousand files be produced. The Court determined that it would not be unduly burdensome for Atlantic City to produce its internal affairs files and thus the Court did not order cost sharing.⁶⁸ The opinion notes, however, that given the expected cost of production, and the well-known facts concerning Atlantic City's dire financial situation, the parties are encouraged to agree upon a reasonable cost-sharing arrangement. Plaintiff's counsel had already indicated a willingness to share costs. The Court noted that the added benefit of requiring the parties to share costs is to encourage the parties to come up with a discovery plan that is time- and cost-efficient.

- 64. Brudnicki, 291 F.R.D. at 676.
- 65. Brudnicki, 291 F.R.D. at 676.
- 66. Brudnicki, 291 F.R.D. at 676.
- 67. Brudnicki, 291 F.R.D. at 676-77.
- 68. Costantino v. City of Atl. City, 152 F. Supp. 3d 311, 336 (D.N.J. 2015).

^{62.} Brudnicki, 291 F.R.D. at 675 (citing Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 284 (S.D.N.Y. 2003) (Zubulake III); Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 322 (S.D.N.Y. 2003) (Zubulake I).

^{63.} Brudnicki, 291 F.R.D. at 676.

Although consensus between the parties is encouraged, counsel should carefully understand the implications of any discovery protocols they enter into before finalizing an agreement. In *Bailey v. Brookdale Univ. Hosp. Med. Ctr.*, No. CV162195AD-SAKT, 2017 WL 2616957, at *1 (E.D.N.Y. June 16, 2017), the parties submitted an ESI agreement, which the court accepted. Afterward, Plaintiff's counsel discovered that in this employment discrimination case he had inadvertently agreed to require his client to bear the costs of certain e-mail recovery costs, and sought relief from the earlier agreed-upon order. The court refused to void the earlier agreement but did alter the cost-sharing arrangement to require defendants to bear forty percent of the costs.

§ 14.2:5 One-Sided Burden of Discovery May Also Provide Basis for Cost Shifting

In cases where discovery is "asymmetrical," some courts have allowed for cost shifting regardless of accessibility of the ESI. In *Boeynaems v. LA Fitness International, LLC*, excessive costs due to asymmetrical discovery, not inaccessibility, was a determining factor in the court's decision to order cost shifting.⁶⁹ In *Boeynaems*, the ESI dispute arose out of "asymmetrical discovery."⁷⁰ The plaintiffs were members of the defendant gym for brief periods of time and alleged they had difficulty canceling their membership.⁷¹ The court noted that the plaintiffs would have few documents (their gym contracts and copies of correspondence), but that the defendant, a large fitness club, could potentially retain millions of items of ESI.⁷² The plaintiff asserted that the defendant's ESI was necessary for the plaintiffs to advocate for class certification pursuant to Federal Rule of Civil Procedure 23.⁷³ Given the asymmetrical posture, the court ultimately shifted the cost of the defendant's ESI production to the plaintiffs, concluding that "economic motivation and fairness" were relevant factors in determining cost shifting of disputed discovery burdens.⁷⁴

The *Boeynaems* court also noted that the plaintiffs were represented by a "very successful and well-regarded" law firm with "outstanding successes" in prosecuting class actions.⁷⁵ Accordingly, the court concluded that if class action counsel "believes that

- 72. Boeynaems, 285 F.R.D. at 334.
- 73. Boeynaems, 285 F.R.D. at 334.
- 74. Boeynaems, 285 F.R.D. at 335.
- 75. Boeynaems, 285 F.R.D. at 335.

325

^{69. 285} F.R.D. 331, 338 (E.D. Pa. Aug. 15, 2012).

^{70.} Boeynaems, 285 F.R.D. at 334.

^{71.} Boeynaems, 285 F.R.D. at 334.

this case is meritorious, it has the financial ability to make the investment in discovery, to the extent the Court finds that cost sharing is otherwise appropriate."⁷⁶ Because the class certification was still pending and the defendant had to date borne all of the costs of complying with discovery, the court concluded that the cost burdens "must

now shift to Plaintiffs, if Plaintiffs believe they need additional discovery."⁷⁷ The court concluded by stating that it was "firmly of the view that discovery burdens should not force either party to succumb to a settlement that is based on the cost of litigation rather than the merits of the case."⁷⁸ As such, the court was willing to shift the cost of discovery to the plaintiffs to avoid the defendant being "force[d] . . . to succumb to a settlement that is based on the cost of litigation."⁷⁹

§ 14.2:6 Cost Shifting May Take Form of Sanctions in Cases of Discovery Abuse

Some courts have held that cost shifting may take the form of sanctions when a party has abused the discovery process. Discovery sanctions serve three purposes: (1) to ensure that a violating party does not benefit from its own failure to comply with discovery; (2) to serve as a specific deterrent to achieve compliance with the particular discovery order at issue; and (3) to serve as a general deterrent in the case at hand and in other litigation, provided that the party against whom sanctions are imposed was in some sense at fault.⁸⁰ Federal Rule of Civil Procedure 37 lists a "menu of possible remedies" for discovery sanctions, the most severe of which include "directing that ... designated facts [in the discovery order] be taken as established for purposes of the action, as the prevailing party claims," to "striking pleadings in whole or in part," or even "dismissing the action or proceeding in whole or in part."⁸¹ A court may also levy monetary sanctions against a violating party in lieu of or in addition to the sanctions outlined in Fed. R. Civ. P. 37(b)(2)(A).⁸² Where a party seeks sanctions for the responding party's failure to produce requested documents, the court "may order pay-

- 76. Boeynaems, 285 F.R.D. at 335.
- 77. Boeynaems, 285 F.R.D. at 341.
- 78. Boeynaems, 285 F.R.D. at 342.
- 79. Boeynaems, 285 F.R.D. at 342.

80. See In re Durand, No. 07-CV-5037 (JFB), 2008 WL 4282601, at *5 (E.D.N.Y. Sept. 16, 2008); see also Gutman v. Klein, No. 03 CV 1570 (BMC)(RML), 2008 WL 4682208, at *11 (E.D.N.Y. Oct. 15, 2008); Klezmer ex rel. Desyatnik v. Buynak, 227 F.R.D. 43, 51 (E.D.N.Y. 2005).

81. See Nycomed U.S. Inc. v. Glenmark Generics, Ltd., No. 08-CV-5023 (CBA)(RLM), 2010 WL 3173785, at *3 (E.D.N.Y. Aug. 11, 2010) (quoting Fed. R. Civ. P. 37(b)(2)(A)).

82. Nycomed, 2010 WL 3173785, at *3 (citing Merck Eprova AG v. Gnosis S.P.A., No. 07 Civ. 5898(RJS), 2010 WL 1631519, at *6 (S.D.N.Y. Apr. 20, 2010)).

ment of the reasonable expenses, including attorney's fees, caused by the failure."⁸³ See chapter 13 of this book.

§ 14.3 Recovering ESI Costs under 28 U.S.C. § 1920

Fed. R. Civ. P. 54(d)(1) provides that "costs—other than attorneys' fees—shall be allowed to the prevailing party." 28 U.S.C. § 1920^{84} sets forth the expenses that may be taxed as costs. Courts are divided regarding what e-discovery charges are recoverable under 28 U.S.C. § 1920(4).⁸⁵

In *Chenault v. Dorel Industries, Inc.*, the prevailing defendant created an electronic database to respond to the plaintiff's discovery requests.⁸⁶ The plaintiff requested all e-mails relating to the ladder at issue in the case, and the defendant's search ultimately yielded an estimated 20,000 e-mails with attachments, which was approximately 800,000 pages.⁸⁷ Although the plaintiff acknowledged that it requested the e-mails in discovery, it argued that the cost of the electronic database was not recoverable and the defendant could have shifted the cost of production by way of objection or by motion seeking a ruling from the court prior to production.⁸⁸ The court noted that the electronic production saved the cost of printing and copying the 800,000 pages, at an estimated cost of \$120,000.⁸⁹ Because the electronic data "was produced in lieu of extremely costly paper production" and the defendant was "seeking to save costs by not printing out thousands of pages of documents, which would have otherwise been required in response" to discovery requests, the court found that the expense fell within the category of costs recoverable for fees and disbursements for printing.⁹⁰

- 88. Chenault, 2010 WL 3064007, at *4.
- 89. Chenault, 2010 WL 3064007, at *4.

90. Chenault, 2010 WL 3064007, at *4; see also Neutrino Development Corp. v. Sonosite, Inc., No. H-01-2484, 2007 WL 998636, at *4 (S.D. Tex. Mar. 30, 2007).

^{83.} Nycomed, 2010 WL 3173785, at *3 (quoting Fed. R. Civ. P. 37(c)(1)(A)).

^{84. 28} U.S.C. § 1920 sets forth the expenses that may be taxed as costs: (1) fees of the clerk and marshal; (2) fees of the court reporter for all or part of the stenographic transcript necessarily obtained for use in the case; (3) fees and disbursements for printing and witnesses; (4) fees for exemplification and copies of papers necessarily obtained for use in the case; (5) docket fees under section 1923 of this title; (6) compensation of court appointed experts, compensation of interpreters, and salaries, fees, expenses, and costs of special interpretation services under section 1828 of this title.

^{85.} See Cofield v. Crumpler, 179 F.R.D. 510, 514 (E.D. Va. 1998).

^{86.} No. A-08-CA-354-SS, 2010 WL 3064007, at *3 (W.D. Tex. Aug. 2, 2010).

^{87.} Chenault, 2010 WL 3064007, at *3.

In *Eolas Technologies, Inc. v. Adobe Systems, Inc.*, the district court considered whether section 1920(4) reached several types of costs that may be generally classified as electronic discovery costs: (1) document scanning, (2) document collection, (3) document processing, (4) document hosting, and (5) conversion to TIFF format.⁹¹ The court concluded that "[d]ocument scanning is essentially copying paper documents to electronic form" and would be a recoverable cost.⁹² The court found that costs for document collection, processing, and hosting were not recoverable costs because section 1920(4) "is not so broad as to cover general electronic discovery costs that precede copying or scanning of materials."⁹³ The court also held that conversion to TIFF, as opposed to production in native format, was not necessary, and thus not a taxable cost.⁹⁴

The Eolas court noted that the Fifth Circuit had not spoken directly to the issue of recovering ESI costs since the statute was amended.95 However, the court was persuaded by the Third Circuit's decision in Race Tires America, Inc. v. Hoosier Racing Tire Corp.⁹⁶ In Race Tires America, the Third Circuit noted that the invoices were "notable for their lack of specificity and clarity as to the services actually performed," including charges for "EDD Processing" and "Performing Searching/Filtering/ Exporting" that did not specify any rationale for the activities or their results in terms of the actual production of discovery material.⁹⁷ Based on the parties' briefing, however, the Court was able to identify general categories of services, including (1) collecting and preserving ESI, (2) processing and indexing ESI, (3) keyword searching of ESI for responsive and privileged documents, (4) converting native files to TIFF, and (5) scanning paper documents to create electronic images.⁹⁸ Likewise, in Vital v. Varco, No. CV H-12-1357, 2015 WL 7740417, at *5 (S.D. Tex. Nov. 30, 2015), aff'd sub nom. Vital v. Nat'l Oilwell Varco, L.P., 685 F. App'x 355 (5th Cir. 2017), the Court declined to award as costs monthly expenses associated with maintaining a database of electronically stored information used to locate, retrieve, and store the plaintiffs' emails.

- 91. 891 F. Supp. 2d 803, 806 (E.D. Tex. 2012).
- 92. Eolas, 891 F. Supp. 2d at 806.
- 93. Eolas, 891 F. Supp. 2d at 806.

94. Eolas, 891 F. Supp. 2d at 807; see also Kellogg Brown & Root International Inc. v. Altannia Commercial Marketing Co. W.L.L., No. H-07-2684, 2009 WL 1457632 (S.D. Tex. May 26, 2009) (declining to award costs for data extraction and storage).

- 95. Eolas, 891 F. Supp. 2d at 806.
- 96. 674 F.3d 158, 169 (3d Cir. 2012), cert. denied, 133 S. Ct. 233 (2012).
- 97. Race Tires America, 674 F.3d at 166-67.
- 98. Race Tires America, 674 F.3d at 167.

The Third Circuit agreed with several other courts that scanning of documents to create digital duplicates and conversion of native files to TIFF, the agreed-on format for production of ESI, constitute "making copies of materials."⁹⁹ However, the court rejected the district court's conclusion that electronic discovery services were allowable costs.¹⁰⁰ The district court had reasoned that the technical services are not the types of services that attorneys or paralegals are capable of providing and remarked that the services were the "21st Century equivalent of making copies."¹⁰¹ The Third Circuit noted that the district court did not explain how all the various services amounted to "making copies," instead "seemingly concluding that, because all the various services were necessary to the ultimate production of electronic 'copies,' the services were equivalent to one entire act of 'making copies."¹⁰² The court noted that courts allowing electronic discovery costs had reasoned that professional services are necessary to the production of intelligible electronic documents and have justified the award by pointing to the efficiencies and costs savings resulting from the electronic discovery consultants.¹⁰³

However, the Third Circuit concluded that decisions allowing all or essentially all electronic discovery consultant charges "are untethered from the statutory moor-ing."¹⁰⁴ The court reasoned:

Section 1920(4) does not state that all steps that lead up to the production of copies of materials are taxable. It does not authorize taxation merely because today's technology requires technical expertise not ordinarily possessed by the typical legal professional. It does not say that activities that encourage cost savings may be taxed. Section 1920(4) authorizes awarding only the cost of making copies.¹⁰⁵

As the Third Circuit noted, even if extensive processing is necessary for production, "that does not mean that the services leading up to the actual production constitute 'making copies."¹⁰⁶ Rather, this processing was analogous to tasks that had to be performed in the pre-digital era to produce documents such as locating paper files and

- 99. Race Tires America, 674 F.3d at 167.
- 100. Race Tires America, 674 F.3d at 168.
- 101. Race Tires America, 674 F.3d at 168.
- 102. Race Tires America, 674 F.3d at 168.
- 103. Race Tires America, 674 F.3d at 168.
- 104. Race Tires America, 674 F.3d at 169.
- 105. Race Tires America, 674 F.3d at 169.
- 106. Race Tires America, 674 F.3d at 169.

collecting, reviewing, and screening the documents.¹⁰⁷ The court noted that those costs have never been recoverable and were not recoverable now because they must be performed by third-party consultants with "technical expertise."¹⁰⁸ The court further noted that courts may not award costs that Congress has not authorized. In the Third Circuit's words, "Congress did not authorize taxation of charges necessarily incurred to discharge discovery obligations. It allowed only for the taxation of the costs of making copies."¹⁰⁹

In *Consumer Financial Protection Bureau v. Weltman, Weinberg & Reis, Co., L.P.A.*, 342 F. Supp. 3d 766 (N.D. Ohio 2018), the court allowed as costs expenses for loading and exporting data into an e-discovery vendor platform as "copying." The opinion further stated that "data conversion, audio transcription, and export of data, all suggest a replication of data that would fit the broader definition of electronic 'copying.'"

In Gonzales v. Pan Am. Labs., L.L.C., No. 3:14-CV-2787-L, 2018 WL 2321896, at *5 (N.D. Tex. May 4, 2018), report and recommendation adopted, No. 3:14-CV-2787-L, 2018 WL 2317749 (N.D. Tex. May 22, 2018), the court rejected costs associated with gathering and hosting data in a platform because "the United States Supreme Court has underscored the 'narrow scope of taxable costs' and has emphasized that 'taxable costs are limited to relatively minor, incidental expenses as is evident from section 1920." (citing *Taniguchi v. Kan Pacific Saipan, Ltd.*, 566 U.S. 560, 573 (2012)). But see Javeler Marine Servs. LLC v. Cross, 175 F. Supp. 3d 756 (S.D. Tex. 2016) (creation of forensic electronic images of defendants' hard drives qualified as "making copies of any materials," as required for expense of creating images to be taxable as cost to employer; forensic electronic images were necessarily obtained for use in the case; but defendants were not entitled to reimbursement for expense of keyword searches).

One judge in the Eastern District of Texas has issued a standing order governing the production of ESI that the court takes into consideration when faced with the issue of cost sharing.¹¹⁰

^{107.} Race Tires America, 674 F.3d at 169.

^{108.} Race Tires America, 674 F.3d at 169.

^{109.} Race Tires America, 674 F.3d at 169; see also Country Vintner of North Carolina, LLC v. E.&J. Gallo Winery, Inc., 718 F.3d 249 (4th Cir. 2013); Structural Metals, Inc. v. S&C Electric Co., No. SA-09-CV-984-XR, 2013 WL 3790450 (W.D. Tex. July 19, 2013).

^{110.} T-Rex Prop. AB v. JCDecaux N. Am., Inc., No. 4:16-CV-303-ALM, 2016 WL 9525603 (E.D. Tex. Sept. 12, 2016).

§ 14.4 Texas Rule of Civil Procedure 196.4

Rule 196.4 of the Texas Rules of Civil Procedure governs requests for production of electronic information.¹¹¹ Pursuant to rule 196.4, if the responding party cannot, through reasonable efforts, retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with the rules.¹¹² If the court orders the responding party to comply with the request, the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to receive and produce the information.¹¹³ The requesting party must specify the data being sought.¹¹⁴ The request is reasonably specific if the responding party understands the scope of the request before the trial court intervenes.¹¹⁵

§ 14.4:1 Rule 196.4 Requires Party to Specifically Identify ESI Sought

In *In re Waste Management of Texas, Inc.*, plaintiff Josh Bray asserted an antitrust action against Waste Management.¹¹⁶ Waste Management produced records responsive to Bray's discovery request in the format of Waste Management's choice, Adobe portable document format (PDF).¹¹⁷ Three years later, Bray requested Waste Management to produce similar information, but this time in its native electronic format with all metadata.¹¹⁸ Bray claimed that the PDF format of the previously produced electronic discovery did not allow comprehensive review of that material.¹¹⁹ Waste Management argued that because Bray failed to specify a form for the electronic discovery as required by the discovery rules, the production in PDF format was reasonable and any "do-over" would be an undue burden.¹²⁰ The court noted that Bray made three requests for electronic discovery before Waste Management produced the documents.¹²¹ While the second request did not contain any definitions or instructions con-

- 117. In re Waste Management, 392 S.W.3d at 865.
- 118. In re Waste Management, 392 S.W.3d at 865.
- 119. In re Waste Management, 392 S.W.3d at 868.
- 120. In re Waste Management, 392 S.W.3d at 873.
- 121. In re Waste Management, 392 S.W.3d at 873.

^{111.} See Tex. R. Civ. P. 196.4.

^{112.} Tex. R. Civ. P. 196.4.

^{113.} Tex. R. Civ. P. 196.4.

^{114.} Tex. R. Civ. P. 196.4.

^{115.} See In re Weekley Homes, L.P., 295 S W.3d 309, 314-15 (Tex. 2009) (orig. proceeding).

^{116. 392} S.W.3d 861, 865 (Tex. App.-Texarkana 2013, orig. proceeding).

cerning electronic discovery, the first and third requests contained the following instruction: "[a]ny and all data or information which is in electronic or magnetic form should be produced in a reasonable manner."¹²² Waste Management cited *Weekley Homes* to argue that requests for production of electronic records must be "clearly understood" so that disputes can be avoided, and Bray's request was not clearly understood.¹²³ The court concluded that the rule does not require the requesting party to specify the exact computer file format.¹²⁴ Rather, a request for "reasonably useable" or a "reasonable manner" is sufficient.¹²⁵ Ultimately, the court concluded that while the second request was not as detailed as Bray's first or third requests, Bray did specify the form of electronic discovery sufficient to comply with the requirements of Texas Rule of Civil Procedure 196.4.¹²⁶

The *Waste Management* court noted that "reasonably useable" or "reasonable manner" provides some needed flexibility to the producing party.¹²⁷ As an example, the court noted that a request for the DOCX file format used by Microsoft Word 2010 might require some producing parties to purchase the specific software requested and expend resources converting files to the requested format.¹²⁸ On the other hand, if the request was simply for "reasonably useable" electronic discovery, the producing party could produce files in WordPerfect X4 format instead and still sufficiently comply with the rule.¹²⁹ The court emphasized that communication between the parties is essential, and, if a party feels a request is too ambiguous, that party should contact the opposing side for further clarification.¹³⁰

In addition to disputing Bray's specificity regarding format of the produced records, Waste Management argued that the cost of converting the PDF records into their native format posed an undue burden on Waste Management.¹³¹ The court stated that a discovery request will not result in an undue burden when the burden of responding to it is the result of the responding party's own "conscious, discretionary decisions."¹³²

- 125. In re Waste Management, 392 S.W.3d at 874.
- 126. In re Waste Management, 392 S.W.3d at 874.
- 127. In re Waste Management, 392 S.W.3d at 874.
- 128. In re Waste Management, 392 S.W.3d at 874.
- 129. In re Waste Management, 392 S.W.3d at 874.
- 130. In re Waste Management, 392 S.W.3d at 874.
- 131. In re Waste Management, 392 S.W.3d at 875.

^{122.} In re Waste Management, 392 S.W.3d at 874.

^{123.} In re Waste Management, 392 S.W.3d at 874 (citing In re Weekley Homes, L.P., 295 S.W.3d 314 (Tex. 2009)).

^{124.} In re Waste Management, 392 S.W.3d at 874.

The court concluded that Texas law is not clear concerning whether a form that removes metadata is a "reasonably useable form."¹³³ As such, the court held that Waste Management made the "conscious decision" to remove metadata and produce the data in PDF format and refused to "rescue Waste Management from potentially costly discretionary decisions."¹³⁴

Rule 196.4 applies similarly in Texas family law cases. In In re M., M. filed an emergency motion for a protective order in which he alleged that one child made an outcry of abuse against the child's mother.¹³⁵ At the hearing, the trial court ordered forensic examination of two cellular phones that had been admitted into evidence during the hearing and ordered M. to pay \$5,000 to W.'s attorney for the services of a forensic examiner.¹³⁶ The order came after an oral motion from W.'s attorney for the forensic examination of the phones.¹³⁷ The court cited rule 196.4 to conclude that the Texas Supreme Court has expressly summarized the proper procedure to obtain discovery of data or information that exists in electronic or magnetic form.¹³⁸ Pursuant to rule 196.4, a proper discovery request must be submitted in writing.¹³⁹ As such, an oral motion for electronic discovery is not a permissible discovery device.¹⁴⁰ In In re M. the phones were admitted into evidence without having first been produced through the normal discovery procedures.¹⁴¹ The court stated that "[g]uiding precedent requires strict compliance first with the rules of discovery to choose the least intrusive means of retrieval, and direct access to another party's electronic storage devices is discouraged."142 Therefore, because the trial court ordered intrusive discovery of the

134. In re Waste Management, 392 S.W.3d at 876.

135. No. 09-12-00179-CV, 2012 WL 1803236, at *1 (Tex. App.—Beaumont May 17, 2012, orig. proceeding) (mem. op.).

^{132.} In re Waste Management, 392 S.W.3d at 875.

^{133.} In re Waste Management, 392 S.W.3d at 876. The court did note that federal authority exists indicating that removal of metadata can render documents not "reasonably usable." In re Waste Management, 392 S.W.3d at 876 (citing Fed. R. Civ. P. 34 advisory committee's note to the 2006 amendments); see, e.g., In re Payment Card Interchange Fee & Merchant Discount, No. MD 05-1720(JG)(JO), 2007 WL 121426, at *3–5, (E.D.N.Y. Jan. 12, 2007) (documents stripped of metadata do not comply with rule 34(b) of the Federal Rules of Civil Procedure); Dahl v. Bain Capital Partners, LLC, 655 F. Supp. 2d 146, 150 (D. Mass. 2009) (spreadsheets must be preduced in native format to be reasonably usable).

^{136.} In re M., 2012 WL 1808236, at *1.

^{137.} In re M., 2012 WL 1808236, at *2.

^{138.} In re M., 2012 WL 1808236, at *2 (citing In re Weekley Homes, 295 S.W.3d at 322).

^{139.} In re M., 2012 WL 1808236, at *2.

^{140.} In re M., 2012 WL 1808236, at *2 (citing In re Weekley Homes, 295 S.W.3d at 315).

^{141.} In re M., 2012 WL 1808236, at *2.

^{142.} In re M., 2012 WL 1808236, at *2.

phones without first having the parties comply with rule 196, the court held that the trial court abused its discretion.¹⁴³

§ 14.4:2 Texas Courts Emphasize "Least Intrusive Means" Must Be Employed to Collect and Review ESI

In In re Pinnacle Engineering, Inc., an employee and shareholder of a privately held corporation sued his former employer for breach of contract, breach of fiduciary duty, shareholder oppression, and other claims after his employment was terminated.¹⁴⁴ Both the employee and the company sought production from each other of documents relating to the employment and stock ownership as well as the production of several computer hard drives.¹⁴⁵ The former employee also sought documents and communications from two other employees and coshareholders of the company ("company custodians").¹⁴⁶ After a series of discovery disputes, the former employee filed a motion to compel the production of forensic images and critical documents in native format with all associated metadata from the company custodians' computers.¹⁴⁷ The trial court ordered that "images" rather than the company custodians' actual computer hard drives be produced.¹⁴⁸ The company custodians sought a writ of mandamus. arguing that the trial court erred in entering the order because the former employee's discovery request did not comply with the specificity requirement of rule 196.4.¹⁴⁹ The former employee's request asked for production of the computer hard drives from the "laptops, desktops, Dell notebooks and tablets" of the employees "from 2009 to 2011."150 The court concluded that these requests did not inform the company custodians of the exact nature of the information sought and, as such, did not meet the requirements of rule 196.4.¹⁵¹ Therefore, the trial court abused its discretion in granting the motion to compel because the former employee's discovery requests did not comport with the requirements of rule 196.4.¹⁵²

150. In re Pinnacle Engineering, 405 S.W.3d at 842.

151. In re Pinnacle Engineering, 405 S.W.3d at 842. (citing In re Jordan, 364 S.W.3d 425, 426 (Tex. App.—Dallas 2012, orig. proceeding) (holding that written requests asking for computer hard drives are insufficient under rule 196.4)).

152. In re Pinnacle Engineering, 405 S.W.3d at 842.

^{143.} In re M., 2012 WL 1808236, at *2 (citing Tex. R. Civ. P. 196).

^{144. 405} S.W.3d 835, 836 (Tex. App.-Houston [1st Dist.] 2013, orig. proceeding).

^{145.} In re Pinnacle Engineering, 405 S.W.3d at 837.

^{146.} In re Pinnacle Engineering, 405 S.W.3d at 837.

^{147.} In re Pinnacle Engineering, 405 S.W.3d at 838.

^{148.} In re Pinnacle Engineering, 405 S.W.3d at 839.

^{149.} In re Pinnacle Engineering, 405 S.W.3d at 841.
The trial court's order also required the company custodians to produce to the former employee's computer expert images from the hard drives of "any computer(s) used" by the former employees, the network servers for the company, and the native files for any document purported to be the former employee's resume.¹⁵³ Pursuant to the Texas Supreme Court's decision in *In re Weekley Homes*, the court noted that "[p]roviding access to information by ordering examination of a party's electronic storage device is particularly intrusive and should be generally discouraged, just as permitted open access to a party's file cabinets for general perusal would be."¹⁵⁴ The court stated:

As a threshold matter, the requesting party must show that the responding party has somehow defaulted in its obligation to search its records and produce the requested data. The requesting party should also show that the responding party's production has been inadequate and that a search of the opponent's [electronic storage device] could recover deleted relevant materials.¹⁵⁵

The *In re Pinnacle Engineering* court noted that the former employee had not presented any evidence that the company custodians' production was inadequate or that a search of their computers and network server hard drives could discover relevant materials.¹⁵⁶ As such, the trial court abused its discretion in compelling the company custodians to turn over their computer and network server hard drives without requiring the former employee to demonstrate that the company custodians had defaulted on their discovery obligations or that their production had been otherwise inadequate.¹⁵⁷

In *In re Clark*, Clark was a former bank officer at Texas Citizens Bank (TCB).¹⁵⁸ During her employment at TCB, she signed a confidential information, nonsolicitation, and noncompetition agreement.¹⁵⁹ A forensic analysis of Clark's work computer revealed that in the final months of her employment, Clark had communicated with representatives of a competitor about opening a branch bank in the same town where Clark was working for TCB.¹⁶⁰ TCB requested production for inspection and copying

^{153.} In re Pinnacle Engineering, 405 S.W.3d at 842.

^{154.} In re Pinnacle Engineering, 405 S.W.3d at 842–43 (quoting In re Weekley Homes L.P., 255 S.W.3d 309, 317 (Tex. 2009)).

^{155.} In re Pinnacle Engineering, 405 S.W.3d at 842–43 (quoting In re Weekley Homes, 295 S.W.3d at 317) (internal citations omitted).

^{156.} In re Pinnacle Engineering, 405 S.W.3d at 844.

^{157.} In re Pinnacle Engineering, 405 S.W.3d at 844 (citing In re Weekley Homes, 295 S.W.3d at 322.

^{158. 345} S.W.3d 209 (Tex. App.-Beaumont 2011, orig. proceeding).

^{159.} In re Clark, 345 S.W.3d at 211.

any and all computers used or accessed by Clark since June 1, 2010.¹⁶¹ In her response, Clark objected to having to produce a personal computer that was used by her family members and that she claimed she did not use for business purposes.¹⁶² Clark claimed she did not take any paper or electronic files with her and that consequently she did not have access to the requested information.¹⁶³ Clark claimed to have no documents stored on any computer in her possession that concerned TCB's customers or operations.¹⁶⁴ She claimed to have no access to any communications with TCB customers or any documents downloaded from a TCB computer.¹⁶⁵ Additionally, she asserted that there were no documents saved on her personal computer that would be relevant to the lawsuit.¹⁶⁶ TCB filed a motion to compel, contending that even if emails had been deleted, artifacts of the sessions would be retrievable from the computer from which the e-mail account had been accessed.¹⁶⁷ At the hearing on the motion to compel, counsel for TCB told the trial court that if Clark's personal computer was surrendered to TCB for a search, its forensic analysts could carve out the surnames of Clark's lawyers as well as the words "attorney" and "lawyer" to ensure that their search of the computer's files did not disclose attorney-client communications.¹⁶⁸ The trial court ordered counsel for Clark to turn over the computer to TCB's counsel by five o'clock that day or face sanctions against both Clark and her counsel.169

As part of its decision, the court noted that the affidavit of TCB's computer forensic analyst demonstrated that partial artifacts of Clark's e-mail sessions had been recovered from the deleted space on Clark's work computer and posited that artifacts and data for deleted e-mails would be visible on the home computer on which Clark admitted she accessed her e-mail account.¹⁷⁰ Accordingly, the court concluded that a forensic analysis of Clark's computer would produce relevant information that has been requested but has not been produced.¹⁷¹ As such, the court concluded that the

- 160. In re Clark, 345 S.W.3d at 211.
- 161. In re Clark, 345 S.W.3d at 211.
- 162. In re Clark, 345 S.W.3d at 211.
- 163. In re Clark, 345 S.W.3d at 211.
- 164. In re Clark, 345 S.W.3d at 211.
- 165. In re Clark, 345 S.W.3d at 211.
- 166. In re Clark, 345 S.W.3d at 211.
- 167. In re Clark, 345 S.W.3d at 212.
- 168. In re Clark, 345 S.W.3d at 212.
- 169. In re Clark, 345 S.W.3d at 212.
- 170. In re Clark, 345 S.W.3d at 212.

trial court could reasonably conclude that Clark's persistence in asserting that she did not produce any electronic data because she had "cleaned" her personal e-mail account demonstrates that she did not adequately search for relevant deleted emails.¹⁷² Accordingly, it was within the trial court's discretion to order the production of electronic information on Clark's personal electronic storage devices.¹⁷³

The appellate court, however, concluded that the trial court failed to protect Clark's sensitive data (particularly attorney-client e-mails) and did not employ the least intrusive means of retrieval.¹⁷⁴ The trial court ordered Clark to produce all of her personal electronic storage devices to TCB.¹⁷⁵ The sole protection directed by the trial court consisted of excluding the surnames of Clark's lawyers and the words "attorney" and "lawyer."¹⁷⁶ No search parameters limited TCB's access to information of a personal and confidential nature that had no possible relevance to the litigation.¹⁷⁷ As such, the trial court's order failed to address privilege, privacy, and confidentiality concerns adequately in accord with *In re Honza*.¹⁷⁸ The appellate court ultimately concluded that allowing TCB's forensic expert to search Clark's personal computer was not the least intrusive means available to determine if relevant information existed on Clark's computer.

§ 14.4:3 Cost Shifting

Assuming that the requesting party has sought relevant ESI and specifically identified the ESI sought, Texas case law is still fairly undeveloped as to when a producing party can request cost shifting. In *In re State Farm Lloyds*, 520 S.W.3d 595, 608 (Tex. 2017), the Court stated that "a particularized need for the proposed discovery will weigh heavily in favor of allowing discovery as requested but, depending on the force of other prudential concerns, may warrant cost shifting for any 'extraordinary steps' required." In a footnote, the Court also stated: "We observe, parenthetically, that the comments to rule 196.4 place the burden of specifying 'any extraordinary steps for

- 176. In re Clark, 345 S.W.3d at 213.
- 177. In re Clark, 345 S.W.3d at 213.

178. In re Clark, 345 S.W.3d at 213 (citing In re Honza, 242 S.W.3d 578, 583-84 (Tex. App.—Waco 2008, orig. proceeding).

^{171.} In re Clark, 345 S.W.3d at 212.

^{172.} In re Clark, 345 S.W.3d at 212.

^{173.} In re Clark, 345 S.W.3d at 212.

^{174.} In re Clark, 345 S.W.3d at 213.

^{175.} In re Clark, 345 S.W.3d at 213.

retrieval and translation' on the requesting party, see Tex. R. Civ. P. 196 cmt. 3, which may necessitate collaborating with the responding party before requesting production of electronic discovery in a particular format." *In re State Farm Lloyds*, at 608, n.44.

§ 14.5 Conclusion

In conclusion, e-discovery is and will continue to be an evolving area of the law that all attorneys must continue to be aware of. Both the Federal and Texas Rules of Civil Procedure allow for procedures for a court to shift costs under certain circumstances. While case law is not entirely settled regarding the circumstances in which courts may order cost shifting or cost sharing, recent cases are illustrative of such circumstances and may be used as a baseline argument to a court that costs should be shifted or shared. Proportionality is a significant factor in determining whether limitations on discovery or shifting of cost should be applied. Moreover, courts appear inclined to prohibit the cost of electronic discovery to be used as a sword to force settlement of litigation, particularly in cases involving asymmetrical discovery. Litigants big or small are entitled to their day in court on the merits of valid disputes, and such a fundamental right must be protected from the cost of big data discovery.

Chapter 15

Spoliation and Sanctions

Judge Xavier Rodriguez

§ 15.1 Introduction

Should a party (or nonparty) fail to comply with discovery preservation obligations and lose or spoliate discovery, that party could face sanctions for its noncompliance. This chapter will focus on the elements of Federal Rule of Civil Procedure 37(e), which addresses the loss of electronically stored information, and the current sanctions analysis under Texas Supreme Court precedent.

§ 15.2 Spoliation or Loss of ESI

§ 15.2:1 Federal Rule of Civil Procedure 37(e) and Inherent Authority

Federal Rule of Civil Procedure 37(e) states the appropriate sanctions for the loss of electronically stored information (ESI) that should have been preserved.

In the 2006 amendments to the Federal Rules of Civil Procedure, rule 37(f) was added, which provided: "Absent exceptional circumstances, sanctions cannot be imposed for loss of electronically stored information resulting from the routine, good-faith operation of an electronic information system." The rule was amended because after 2006 the various federal courts established significantly different standards for imposing sanctions or curative measures on parties who failed to preserve electronically stored information. The rule advisory committee was also concerned that litigants were expending "excessive effort and money on preservation in order to avoid the risk of severe sanctions if a court finds they did not do enough."

Current rule 37(e), which became effective December 1, 2015, displaces the 2006 rule. This is an important point. There is much confusion in the case law because litigants and courts continue to cite to cases interpreting the 2006 rule. Practitioners should be wary when relying on or citing to any cases decided before December 1, 2015, when analyzing this area of the law.

The current version of Federal Rule of Civil Procedure 37(e) reads as follows:

Fed. R. Civ. P. 37(e) Failure to Preserve Electronically Stored Information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

- upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
- (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
 - (A) presume that the lost information was unfavorable to the party;
 - (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
 - (C) dismiss the action or enter a default judgment.

According to the advisory committee note, rule 37(e) "forecloses reliance on inherent authority or state law to determine when certain measures should be used."¹ Federal courts possess certain "inherent powers," not conferred by rule or statute, to manage their own affairs so as to achieve the orderly and expeditious disposition of cases. That authority includes "the ability to fashion an appropriate sanction for conduct that abuses the judicial process."²

Notwithstanding the language in the advisory committee note, some federal courts have continued to issue sanctions exercising the court's inherent authority.³ These courts recognize that a court must exercise its inherent powers "with restraint and dis-

^{1.} Fed. R. Civ. P. 26(e) 2015 advisory committee's note.

^{2.} Goodyear Tire & Rubber Co. v. Haeger, 137 S. Ct. 1178, 1186 (2017) (citations omitted).

^{3.} See, e.g., Ottoson v. SMBC Leasing & Fin., Inc., 268 F. Supp. 3d 570, 580 (S.D.N.Y. 2017) ("In addition [to rule 37(e)], the court may impose discovery sanctions pursuant to 'its inherent power to manage its own affairs."); Davis v. Hinds Cty., Mississippi, No. 3:16-CV-674-DPJ-FKB, 2018 WL 4656304, at *5 (S.D. Miss. Sept. 27, 2018) ("Court has the authority to sanction a party for misrepresentations and for discovery misconduct..."); Hsueh v. New York State Dep't of Financial Services, No. 15 Civ. 3401, 2017 WL 1194706 (S.D.N.Y. Mar. 31, 2017) (Plaintiff deleted recording she made with HR representative). In Quantlab Techs. Ltd. (BVI) v. Godlevsky, 317 F. Supp. 3d 943, 947 (S.D. Tex. 2018), the court granted attorney's fees in excess of \$3 million because the defendants failed "to conduct themselves with any measure of honesty, responsibility, or good faith." See also Klipsch Grp., Inc. v. ePRO E-Commerce Ltd., 880 F.3d 620, 632 (2d Cir. 2018) (affirming sanctions and amount of award even though the actual amount in controversy was small).

Spoliation and Sanctions

cretion," but may look to its inherent power "to fill in the interstices" not covered by the rules or a statute.⁴

The Supreme Court has not definitely settled whether rule 37(e) precludes sanctions issued under inherent authority, but the Court has stated that any measures imposed under the court's inherent authority must be compensatory rather than punitive in nature. "In other words, the fee award may go no further than to redress the wronged party 'for losses sustained'; it may not impose an additional amount as punishment for the sanctioned party's misbehavior." *Goodyear Tire & Rubber Co. v. Haeger*, 137 S. Ct. 1178, 1186 (2017).

Some courts have considered rule 37 but recognized that because of a unique fact pattern the rule could not be applied and have accordingly issued sanctions under the court's inherent authority. For example, in *United States ex rel. Scutellaro v. Capitol Supply, Inc.*, the defendant had obligations to maintain various documents pursuant to government regulations. The documents were not required to be kept because there was no anticipated litigation at the time, and accordingly rule 37 did not apply. Nevertheless, the court gave an adverse jury instruction because there was "no question that the spoliated COO information would constitute direct proof or disproof of the falsity of claims made to the government."⁵

Other courts have simply addressed the issue of sanctions without any reference to rule 37.⁶ The Third and Ninth Circuits have expressly cautioned judges to apply rule 37.⁷ Inasmuch as rule 37(e) only applies to ESI, courts deciding the question of loss of non-ESI have relied upon the court's inherent authority.⁸

7. See Newberry v. Cty. of San Bernardino, 750 F. App'x 534 (9th Cir. Sept. 18, 2018) ("Rule 37(e) 'therefore foreclose[d] reliance on inherent authority' to determine whether terminating sanctions were appropriate."); Clientron Corp. v. Devon IT, inc., 894 F.3d 568, 577 (3d Cir. 2018) ("Our 'preferred' course, however, is that when 'statutory or rules-based sanctions are entirely adequate, they should be invoked, rather than the inherent power."").

^{4.} Johnson v. Ford Motor Co., No. CV 3:13-6529, 2017 WL 6614101, at *2 (S.D. W. Va. Dec. 27, 2017), reh'g granted [denied in part], No. CV 3:13-6529, 2018 WL 1512376 (S.D. W. Va. Mar. 26, 2018) (Ford ordered to pay almost \$500,000 in fees and expert costs.).

^{5.} No. CV 10-1094 (BAH), 2017 WL 1422364, at *11 (D.D.C. Apr. 19, 2017).

^{6.} See Bryant v. Wal-Mart Louisiana, L.L.C., 729 F. App'x 369, 370 (5th Cir. 2018) ("A district court's decision regarding sanctions for spoliation is reviewed for an abuse of discretion. 'An adverse inference based on the destruction of potential evidence is predicated on the 'bad conduct' of the defendant.' That generally requires evidence of 'bad faith.' The district court concluded that Wal-Mart did not act in bad faith in deleting videos because (1) none of the videos showed the relevant area where the fall occurred, and (2) Wal-Mart deleted the videos showing other parts of the store pursuant to a standardized retention policy."). In United States v. Regents of New Mexico State Univ., No. 16-CV-911-JAP-LF, 2018 WL 3719240, at *2 (D.N.M. Aug. 3, 2018), without reference to rule 37 and apparently relying on inherent authority, the court ordered evidence preclusion as a sanction for the failure to keep certain records.

Confusingly, many courts are issuing orders that fail to cite to rule 37 and analyze the case under pre-2015 cases.⁹

§ 15.2:2 Analyzing Federal Rule of Civil Procedure 37(e)

When analyzing rule 37(e), all elements of the prefatory paragraph must be established before reviewing whether (e)(1) or (e)(2) is applicable.

"If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery"¹⁰

§ 15.2:3 Rule 37(e) Applies Only to ESI

Rule 37(e) applies to the loss of ESI, so courts continue to use circuit common law when the loss of paper documents or non-ESI occur. See World Trade Centers Ass'n, Inc. v. Port Auth. of New York & New Jersey, No. 15CIV7411LTSRWL, 2018 WL 1989616, at *7 (S.D.N.Y. Apr. 2, 2018), report and recommendation adopted sub nom. World Trade Centers Ass'n v. Port Auth. of New York & New Jersey, No. 15 CV 7411-LTS-RWL, 2018 WL 1989556 (S.D.N.Y. Apr. 25, 2018).

§ 15.2:4 ESI That Should Have Been Preserved

"A court must first determine when the duty to preserve evidence was triggered, and what evidence should have been preserved. 'The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.' Proper analysis of the question of what evidence must be preserved 'requires the Court to determine reasonableness under the circumstances.'"¹¹ See also Chapter 1—Duty to Preserve.

^{8.} See Gipson v. Mgmt. & Training Corp., No. 3:16-CV-624-DPJ-FKB, 2018 WL 736265, at *7 (S.D. Miss. Feb. 6, 2018).

^{9.} See, e.g., Satterfield v. Chipotle Mexican Grill, Inc., No. 15 C 10308, 2017 WL 1283461, at *1 (N.D. Ill. Apr. 6, 2017).

^{10.} Fed. R. Civ. P. 37(e).

^{11.} Ballard v. Wal-Mart Stores East, LP, No. 5:17-CV-03057, 2018 WL 4964361, at *2 (S.D. W. Va. Oct. 15, 2018); ILWU-PMA Welfare Plan Bd. of Trustees & ILWU-PMA Welfare Plan v. Connecticut Gen. Life Ins. Co., No. C 15-02965 WHA, 2017 WL 345988, at *1 (N.D. Cal. Jan. 24, 2017) (Carewise executed a tolling agreement contemplating claims in connection with "benefits paid out under the Plan" or "breaches of contractual or other obligations owed between and among the Parties.").

Spoliation and Sanctions

An argument that defendants should have preserved certain data because they generally knew their facility had environmental problems was rejected by the trial court as satisfying the threshold that litigation was reasonably anticipated.¹² Vague telephone statements by a plaintiff who told a manager that she fell "in the front end of the store near the cash registers that afternoon" have been found not to trigger a preservation obligation, especially since the statement was insufficiently precise to alert the store to what evidence it should have preserved. Moreover, the statement neither threatened nor referenced litigation, and she never filed a formal complaint.¹³

"[T]he phrase 'should have been preserved' encompasses the concept of the duty to preserve ESI. If there were no duty to preserve the ESI, then it need not have been preserved. Moreover, this provision appears to be based on a prospective standard. Using hindsight to determine that the ESI 'should have been preserved' is far too easy. Accordingly, the better interpretation of this provision is that the determination of what ESI 'should have been preserved' is viewed at the time litigation is anticipated or ongoing, not when it is discovered that the ESI was lost. And this prospective standard is from the viewpoint of the party who controls the ESI. Finally, this provision limits the preservation to only relevant ESI."

In *In re Abilify (Aripiprazole) Prod. Liab. Litig.*, the court rejected the plaintiffs' argument that the defendant should have reasonably anticipated litigation because of information disclosed in publications and other lawsuits concerning other drugs, and based on information OAPI received in adverse event reports.¹⁵

In a confusing opinion, one court excused a plaintiff's failure to keep text messages from his cell phone (after he had expressed comments about initiating legal action),

15. No. 3:16-MD-2734, 2018 WL 4856767, at *3 (N.D. Fla. Oct. 5, 2018) ("Certainly, nothing Plaintiffs did before these cases were filed or anything that any of Plaintiffs'respective counsel did before these cases were filed evidence that OAPI could have or should have reasonably anticipated litigation in the 2002 to 2006 time frame. Plaintiffs' counsel did not begin advertising for plaintiffs in this litigation until 2013 and did not threaten OAPI with litigation until October 2014, more than a decade after the emails were deleted. Indeed, the first lawsuit involving Abilify was not filed until January 2016. Thus, the earliest date OAPI should have reasonably anticipated litigation is when it first learned that claims might be filed, either as early as 2013, but not later than October 2014, when OAPI was threatened with litigation.").

^{12.} A.O.A. v. Rennert, No. 4:11 CV 44 CDP, 2018 WL 1251827, at *4 (E.D. Mo. Mar. 12, 2018).

^{13.} Washington v. Wal-Mart Louisiana LLC, No. CV 16-1403, 2018 WL 2292762, at *4 (W.D. La. May 17, 2018).

^{14.} Snider v. Danfoss, LLC, No. 15 CV 4748, 2017 WL 2973464, at *4 (N.D. Ill. July 12, 2017), report and recommendation adopted, No. 1:15-CV-04748, 2017 WL 3268891 (N.D. Ill. Aug. 1, 2017) (finding that a duty to preserve emails existed and defendant "mechanically and blindly followed its 90-day destruction policy in the face of a clear threat of litigation").

relying upon the 2015 advisory committee note that courts should be sensitive to the party's sophistication with regard to litigation in evaluating preservation efforts.¹⁶

§ 15.2:5 Failure to Take Reasonable Steps to Preserve

In *Small v. University Medical Center*, UMC and its counsel took no steps to put a litigation hold¹⁷ in place until April 15, 2013, when it then sent an inadequate e-mail providing "little or no guidance to key custodians about what the case was about and what evidence should be preserved." The litigation hold failed to notify key custodians and IT staff responsible for maintaining data of the need to preserve and prevent destruction until months after the special master was appointed. UMC and its counsel failed to conduct an adequate investigation to determine which employees were likely to have discoverable information and where that information was stored. UMC executives and its counsel failed to instruct any UMC employees to suspend any automatic data destruction policies.¹⁸ Similarly, in *Moody v. CSX Transportation, Inc.*, the court found that failure to access or review the data at any time during a four-year period indicated a failure to take reasonable steps.¹⁹

In a case where the party argued that it lost data as a result of a software attack, the court took the rule 37 sanctions motion under advisement until time of trial to determine whether the party took reasonable steps to preserve the information before the cyberattack.²⁰

Companies oftentimes allow (or at least tolerantly ignore) their employees' usage of private messaging systems for business purposes. Failure to maintain a software usage policy²¹ requiring employees to segregate personal and business accounts or to otherwise ensure that professional communications sent through personal accounts can be

20. W. Power, Inc. v. TransAmerican Power Prod., Inc., 316 F. Supp. 3d 979, 997 (S.D. Tex. 2018).

21. See Chapter 2-Litigation Holds.

^{16.} *Trainer v. Cont'l Carbonic Prod., Inc.*, No. 16-CV-4335 (DSD/SER), 2018 WL 3014124, at *4 (D. Minn. June 15, 2018).

^{17.} See Chapter 2-Litigation Holds.

^{18.} Small v. Univ. Med. Ctr., No. 2:13-CV-0298-APG-PAL, 2018 WL 3795238, at *60–61 (D. Nev. Aug. 9, 2018). See also EPAC Techs., Inc. v. HarperCollins Christian Publ'g, Inc., No. 3:12-CV-00463, 2018 WL 1542040, at *22 (M.D. Tenn. Mar. 29, 2018), aff'd as modified sub nom. EPAC Techs., Inc. v. Thomas Nelson, Inc., No. 3:12-CV-00463, 2018 WL 3322305 (M.D. Tenn. May 14, 2018) (faulting counsel for failure to take an active and primary role in implementing a litigation hold); Lokai Holdings LLC v. Twin Tiger USA LLC, No. 15CV9363 (ALC) (DF), 2018 WL 1512055, at *11 (S.D.N.Y. Mar. 12, 2018) (small business and its counsel not excused from taking reasonable steps to preserve e-mail).

^{19. 271} F. Supp. 3d 410, 426 (W.D.N.Y. 2017).

Spoliation and Sanctions

§ 15.2:6 ESI Cannot be Restored or Replaced through Additional Discovery

In *Barcroft Media, Ltd. v. Coed Media Grp., LLC*, the court summarily denied the plaintiffs' sanctions motion where the plaintiffs themselves possessed copies of the web pages at issue—in the form of screen captures taken.²³

In *Steves & Sons, Inc. v. JELD-WEN, Inc.*, the court placed the burden on the movant to show that the lost ESI cannot be replaced or restored. "This factor does not require that JELD-WEN pursue every possible avenue for replacing or restoring the ESI, but it must show that it made some good-faith attempt to explore its alternatives before pursuing spoliation sanctions."²⁴

§ 15.2:7 Intentional Spoliation or Negligent Loss

Assuming all the prefatory elements of rule 37(e) have been established, the proponent of a rule 37(e) motion must decide whether it can establish that the loss of ESI was due to an intent to deprive the requesting party of data, or whether the loss was due to an inadvertent act.

§ 15.2:8 Rule 37(e)(1) Prejudice

"[U]pon finding *prejudice* to another party from loss of the information, [the court] may order measures no greater than necessary to cure the prejudice" (emphasis added). Fed. R. Civ. P. 37(e)(1).

Assuming the loss of data was due to unintentional conduct, a party must still first establish that it was prejudiced by the loss of data.

Obviously, establishing prejudice is tricky business. All involved—the court, the party that failed to preserve, and the seeking party—are at a disadvantage because none know precisely what the lost ESI contained or

^{22.} Klipsch Grp., Inc. v. ePRO E-Commerce Ltd., 880 F.3d 620, 629 (2d Cir. 2018).

^{23.} No. 16-CV-7634 (JMF), 2017 WL 4334138, at *1 (S.D.N.Y. Sept. 28, 2017).

^{24. 327} F.R.D. 96, 109 (E.D. Va. 2018).

showed. It is difficult for a court to determine prejudice when the ESI no longer exists and cannot be viewed. Likewise, it is difficult for the party that failed to preserve the ESI to show the absence of prejudice, again because the ESI was lost. Of course, this party is inclined to minimize the prejudice and importance of the lost ESI. And similarly, it is difficult for the party that seeks the ESI to establish prejudice because it does not know what was contained in the ESI. This party is predisposed to over emphasize the prejudice and importance of the lost ESI. The advisory committee notes recognize this dilemma but offer no solutions To evaluate prejudice, the court must have some evidence regarding the particular nature of the missing ESI.

Snider v. Danfoss, LLC, No. 15 CV 4748, 2017 WL 2973464 at *7 (N.D. Ill. July 12, 2017).²⁵

Some parties have attempted to argue that the loss of e-mails could not be prejudicial because "there are other means to obtain the contents of the conversations from the defendants, including prior oral discovery and potential trial testimony."²⁶ At least one court has rejected such arguments by stating—

A party has the right to prosecute its case in the way it deems fit based on all available relevant evidence. The content of text messages cannot be replaced simply by eliciting testimony from the Defendants, and by having Plaintiff accept that testimony rather than relying on the actual messages to use as they deem fit. Without the lost text messages, Plaintiff is deprived of the opportunity to know 'the precise nature and frequency' of those private communications, which occurred during a critical time period.²⁷

Likewise, in Kische USA LLC v. Simsek, the court stated-

[W]here e-mails and documents are missing entirely due to a party's failure to preserve and their relevance cannot be directly ascertained, "a party

^{25.} Concluding that no prejudice existed because "e-mails not only to and from the human resources department were preserved and produced, but also that Danfoss preserved and has produced to the Court all of Rick White's e-mails to and from Ms. Blood and Plaintiff during the relevant time period As to Plaintiff's deleted e-mails, Plaintiff is obviously a party to the suit and has firsthand knowledge of the substance of e-mails she sent or received [I]f the case goes to trial, she can testify as to any e-mails at that time, assuming the testimony is admissible. Accordingly, no prejudice exists as to Plaintiff's e-mails."

^{26.} Schmalz v. Vill. of N. Riverside, No. 13 C 8012, 2018 WL 1704109, at *4 (N.D. III. Mar. 23, 2018).

^{27.} Schmalz, 2018 WL 1704109, at *4.

'can hardly assert any presumption of irrelevance to the destroyed documents.'" Rather, the party that fails to preserve evidence "bear[s] the consequence of [the] uncertainty" as to the relevance of the documents and the resulting prejudice."²⁸

It is oftentimes difficult to ascertain prejudice when a party does not fully understand what has been lost. In a section 1983 case where the plaintiff lost video that resided on his cell phone, the defendants argued that the lost video "was the best evidence of the presence and location of [Rochester's] gun, as well as critical events that led to plaintiffs' arrest." The court disagreed, stating: "But that assertion is pure speculation; Defendants do not actually know what (if anything) was filmed by Simon, let alone whether it would have been helpful to their case. Even assuming arguendo that the video did capture the location of Rochester's gun, it would be largely irrelevant to the question of whether Defendants had probable cause to arrest Plaintiffs."29 Likewise, in Alston v. City of Darien, the Eleventh Circuit affirmed the trial court's grant of summary judgment in an excessive force case because the plaintiff failed to show that he was prejudiced by the absence of dashcam video. Alston argued that the video "would speak for itself and would either exonerate appellee Brown or show the extent of his unlawful behavior. Alston's concession that the video might exonerate Brown fails to demonstrate the necessary prejudice. Moreover, Alston testified about what happened on the scene of the arrest and during his transport to the jail."³⁰

At least two courts have stated: "[P]rejudice exists where documents that are relevant to a claim are unavailable and the moving party has come forward with a plausible, good faith suggestion as to what the evidence might have been."³¹ The 2015 advisory committee notes to rule 37(e) explain that "[a]n evaluation of prejudice from the loss of information necessarily includes an evaluation of the information's importance in the litigation."

Some courts have concluded that requiring too much from a requesting party to establish prejudice is unfair.³²

31. Sinclair v. Cambria Cty., No. 3:17-CV-149, 2018 WL 4689111, at *2 (W.D. Pa. Sept. 28, 2018).

^{28.} No. C16-0168JLR, 2018 WL 620493, at *5 (W.D. Wash. Jan. 29, 2018) (issuing an adverse jury instruction and prohibiting Defendants from introducing despoiled or improperly withheld evidence at trial, because "Defendants cannot utilize at trial evidence that they currently claim does not exist.").

^{29.} Simon v. City of New York, No. 14-CV-8391 (JMF), 2017 WL 57860, at *7 (S.D.N.Y. Jan. 5, 2017) (citing Goldrich v. City of Jersey City, No. 15-885, 2018 WL 4492931, at *10 (D.N.J. July 25, 2018)).

^{30.} Alston v. City of Darien, 750 F. App'x 825, 835 (11th Cir. 2018).

§ 15.2:9 Rule 37(e)(1) Curative Measures No Greater than Necessary

Even when a party moving for rule 37(e)(1) relief establishes that it has been prejudiced by the loss of ESI, federal trial courts are instructed to award curative measures (not sanctions) no greater than necessary.

In *Small v. Univ. Med. Ctr.*, a case where it appears the court issued relief under rule 26(e)(1), the court rejected a special master's recommendation for granting a default judgment in favor of the plaintiffs because of defendant's willful, bad faith conduct. The court instead assessed costs and attorney's fees and stated that it would include an adverse inference jury instruction.³³ Arguably, this relief is improper under 37(e)(1) as an adverse jury instruction is to be limited to rule 37(e)(2) cases.³⁴

In another case, one party successfully argued that a permissive adverse jury instruction should be issued to the jury to allow her to testify in front of the jury as to why she had discarded certain files.³⁵ Some courts have ordered that the negligent party be prevented from introducing certain evidence at trial.³⁶

Some parties have objected that a court failed to issue strong enough curative factors when discovery obligations were not met. In *Barbera v. Pearson Educ., Inc.*, the court

^{32.} Moody v. CSX Transportation, Inc., 271 F. Supp. 3d 410, 430 (W.D.N.Y. 2017) ("[E]vent recorder data would have conclusively determined whether the horn or bell on Train Q627 were sounded prior to movement. That critical and irreplaceable data was within defendants' complete control to review and produce, but they failed to take simple, reasonable steps to preserve it. Moody has identified testimonial evidence (her own and that of her friend Tiffany Johnson) that the bell and/or horn were not sounded prior to train movement. Under these circumstances, it is plausible that the data from the event recorder would have supported Moody's case. Accordingly, prejudice has been established.").

^{33.} No. 2:13-CV-0298-APG-PAL, 2018 WL 3795238, at *71 (D. Nev. Aug. 9, 2018) ("[T]he court has found UMC failed to comply with its legal duty to preserve discoverable information, failed to comply with its discovery obligations, and failed to comply with a number of the court's orders. The instruction will provide that these failures resulted in the loss or destruction of some ESI relevant to the parties' claims and defenses and responsive to plaintiffs' discovery requests, and that the jury may consider these findings with all other evidence in the case for whatever value it deems appropriate.").

^{34. &}quot;Care must be taken, however, to ensure that curative measures under subdivision (e)(1) do not have the effect of measures that are permitted under subdivision (e)(2) only on a finding of intent to deprive another party of the lost information's use in the litigation." Fed. R. Civ. P. 26(e) 2015 advisory committee's note.

^{35.} Cordoba v. Pulido, No. C 12-4857 (PR), 2018 WL 500185, at *3 (N.D. Cal. Jan. 21, 2018) ("[P]ermitting Defendant to explain her reasons for destroying the Kelley file is appropriate to assist the jury in its determination of whether it should infer that the file contained information unfavorable to Defendant.").

^{36.} Leidig v. Buzzfeed, Inc., No. 16CIV542VMGWG, 2017 WL 6512353, at *13 (S.D.N.Y. Dec. 19, 2017); Hugler v. Sw. Fuel Mgmt., Inc., No. 16CV4547FMOAGRX, 2017 WL 8941163, at *12 (C.D. Cal. May 2, 2017).

found that the employer had negligently destroyed e-mails, but only ordered that Pearson could not contest Barbera's recollection of the e-mails. Further, the magistrate judge held that any prejudice could be cured by requiring certain stipulations of fact—concerning the contents of the e-mail exchange—be taken as true. The court of appeals affirmed.³⁷ Likewise, in *ML Healthcare Servs., LLC v. Publix Super Markets, Inc.*, the Eleventh Circuit found the district court did not abuse its discretion by concluding that defendant's failure to retain more video did not constitute bad faith or demonstrate an intent to deprive plaintiff of evidence necessary to her case. "Defendant immediately saved the most relevant portion of the video—the hour during which Plaintiff's fall occurred, which covered the entire time Plaintiff was in the store—before any request for preservation or notice of litigation was provided."³⁸

§ 15.2:10 Are Attorney's Fees Recoverable to a Prevailing Party?

"Notably absent from rule 37(e) is the mention of attorneys' fees as a sanction, either for having to file the motion or for the failure to preserve the ESI. And the advisory committee notes are shockingly silent on the issue as well. In fact, the minutes of the advisory committee meetings reflect that those in attendance recognized this absence, but simply chose not to do anything about it."³⁹ Notwithstanding the absence of language, many courts continue to award attorney's fees and costs associated with the discovery failure.⁴⁰

§ 15.2:11 Rule 37(e)(2) Intent to Deprive

(2) only upon a finding that the party acted with the *intent to deprive* another party of the information's use *in the litigation* may:

39. Snider v. Danfoss, LLC, No. 15 CV 4748, 2017 WL 2973464, at *5 (N.D. III. July 12, 2007).

40. See Sinclair v. Cambria Cty., No. 3:17-CV-149, 2018 WL 4689111, at *3 (W.D. Pa. Sept. 28, 2018); Lokai Holdings LLC v. Twin Tiger USA LLC, No. 15CV9363 (ALC) (DF), 2018 WL 1512055, at *17 (S.D.N.Y. Mar. 12, 2018).

^{37. 906} F.3d 621 (7th Cir. 2018).

^{38. 881} F.3d 1293, 1308 (11th Cir. 2018) ("Likewise, the district court did not abuse its discretion by denying Plaintiff's alternative sanctions request, which was to preclude Defendant's witnesses from testifying that the location of Plaintiff's fall had been cleaned or inspected hours prior to the accident In both its initial ruling and its oral ruling upon reconsideration, the district court held that Plaintiff had not been prejudiced by Defendant's failure to provide additional video evidence. Specifically, the court found that any additional benefit from the undisclosed video was 'purely speculation and conjecture,' and that the resolution of the videos was not clear enough to see any liquids on the floor, even if the videos were available. The court thus concluded that 'having additional videotape to look at would accomplish nothing but consume more of everybody's time in this case.' There is no basis for finding that the district court abused its discretion in reaching this conclusion.").

- (A) presume that the lost information was unfavorable to the party;
- (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
- (C) dismiss the action or enter a default judgment.

Fed. R. Civ. P. 37(e)(2) (emphasis added).

A plaintiff must present evidence that the defendant destroyed the ESI with an intent to deprive the plaintiff of this ESI.⁴¹ An individual's spoliation may be imputed to a defendant where that person is acting within the scope of his employment.⁴² In cases where intent to deprive has been established, the typical sanction has been to give the jury a permissive adverse inference instruction.⁴³ One court also ordered that the spoliator's external hard drive be subject to a forensic examination as a sanction.⁴⁴ Intentional use of wiping tools evidences an intent to deprive.⁴⁵ Otherwise, courts continue to struggle with whether circumstantial evidence may allow an inference of intent to deprive.⁴⁶ The Eighth Circuit has suggested that circumstantial evidence can establish an intent to deprive and that a "smoking gun" is not required, but nevertheless more is required than negligent conduct.⁴⁷ Some courts have required that an intent finding be based on clear and convincing evidence.⁴⁸ Other courts, including those in the Fifth Circuit, have suggested that "bad faith" must be established.⁴⁹

For a case illustrating how difficult it has been to secure sanction in courts in the Fifth Circuit, see *Orchestratehr, Inc. v. Trombetta*, 178 F. Supp. 3d 476, 493 (N.D. Tex. 2016), *objections overruled*, No. 3:13-CV-2110-KS-BH, 2016 WL 5942223 (N.D. Tex. Oct. 13, 2016) ("In his deposition, Mr. Trombetta admitted that he deleted e-mails and that he 'may' have done so to 'cover his tracks.' In his declaration, how-

^{41.} Snider v. Danfoss, LLC, No. 15 CV 4748, 2017 WL 2973464, at *8 (N.D. Ill. July 12, 2017) ("Plaintiff has presented no evidence that Danfoss destroyed the e-mails with the intent to deprive Plaintiff of this ESI. Instead, what little evidence presented on the issue of intent indicates that Danfoss acted with a pure heart but empty head."); Jackson v. Haynes & Haynes, No. 2:16-cv-018-AKK 2017 WL 3173302 (N.D. Ala. July 26, 2017) (ESI on smartphone not retained by plaintiff. Court found negligence and irresponsible not sufficient to establish intent to deprive.); Archer v. York City Sch. Dist., 710 F. App'x 94, 101 (3d Cir. 2017) ("[N]o evidence to show that the District intentionally deleted the account of the assistant superintendent to destroy evidence, or that the e-mail account would have contained any relevant evidence at all. Given that test scores are the linchpin of the Defendants' defense, and there is no argument that the assistant superintendent would have had any involvement in the statistical results produced by a state-wide, state-administered academic test, the spoliation argument is particularly weak."); Organik Kimya, San ve Tic. A.S. v. Int'l Trade Comm'n, 848 F.3d 994 (Fed. Cir. 2017) (Plaintiffs intentionally began overwriting their laptops to delete relevant files days before an investigation. Rule 37(e) applied not only to penalize, but to deter others who may be tempted to engage in similar misconduct.).

^{42.} RealPage, Inc. v. Enter. Risk Control, LLC, No. 4:16-CV-00737, 2017 WL 3313729, at *12 (E.D. Tex. Aug. 3, 2017).

Spoliation and Sanctions

ever, he states that he deleted e-mails in the ordinary course of business only, and even though he admits that he forwarded some e-mails to his personal Hotmail account, he testifies that those e-mails have been produced to Plaintiffs in this litigation. Considering the totality of the circumstances concerning Mr. Trombetta's deletion of e-mails on the eve of his departure from Orchestrate, including Mr. Trombetta's conflicting and (even considering only his deposition) equivocal testimony on the issue, the Court finds that Plaintiffs have failed to show that Mr. Trombetta destroyed any emails in bad faith or with the requisite intent to deprive Plaintiffs of the use of them in this litigation. Even though the evidence is troubling—Mr. Trombetta gave evasive answers at his deposition, only to provide more definite statements in a later-created declaration—because the supporting evidence of intent or bad faith is not sufficient, the Court concludes that sanctions should not, as Plaintiffs request, be imposed.").

44. TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo, No. CV 15-2121 (BJM), 2017 WL 1155743, at *3 (D.P.R. Mar. 27, 2017).

45. In re Correra, 589 B.R. 76, 136 (Bankr. N.D. Tex. 2018). But see HCC Ins. Holdings, Inc. v. Flowers, 2017 WL 393732 (N.D. Ga. Jan. 30, 2017) (No evidence of actual prejudice shown even though defendant ran several computer cleaning programs on his laptop after a court ordered production.).

^{43.} See GN Netcom, Inc. v. Plantronics, Inc., No. CV 12-1318-LPS, 2017 WL 4417810, at *4 (D. Del. Oct. 5, 2017) ("Despite the direction from Plantronics to preserve documents, after receiving the hold notices, Mr. Don Houston-who was then the Senior Vice President of U.S. Commercial Sales for Plantronics-deleted certain e-mails and, on three occasions, directed others to delete certain e-mails."); E.E.O.C. v. GMRI, Inc., No. 15-20561-CIV, 2017 WL 5068372, at *31 (S.D. Fla. Nov. 1, 2017); TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo, No. CV 15-2121 (BJM), 2017 WL 1155743, at *3 (D.P.R. Mar. 27, 2017); Waymo LLC v. Uber Techs., Inc., No. C 17-00939 WHA, 2018 WL 646701, at *23 (N.D. Cal. Jan. 30, 2018) ("First, the Court itself will inform the jury that, despite the expedited discovery and provisional relief orders, Uber failed to timely disclose the destruction of the five discs and repeatedly supplemented both its communications log and accounting after the ordered deadlines. The Court will instruct the jury that it may, but need not, draw any adverse inference from these facts, and will further explain that the nature of any adverse inference likewise remains up to the jury. ... Second, as explained above, evidence of Uber's litigation misconduct or corporate culture may be relevant and admissible insofar as it reasonably bears on the merits of this case. This includes evidence and argument that Waymo has been unable to find stronger proof of its claims due to Uber's obstruction tactics. But such evidence will not be allowed to consume the trial to the point that it becomes a distraction from the merits or turns into a public exercise in character assassination. Again, the point is to maintain a fair balance between allowing Waymo to reasonably explain any weaknesses in its case on the one hand, and preventing Waymo from sidestepping its burden of proof by inflaming the jury against Uber on the other."); Goldrich v. City of Jersey City, No. CV15885SDWLDW, 2018 WL 4489674, at *2 (D.N.J. Sept. 19, 2018); Edelson v. Cheung, 2017 WL 150241 (D.N.J. Jan. 12, 2017) (Court awarded adverse jury instruction against the defendant for deleting e-mails from his computer. Defendant had opened a second e-mail account, which he did not disclose for the purpose of evading discovery, and then deleted key emails when the account was discovered.); GoPro, Inc. v. 360Heros, Inc., No. 16-CV-01944-SI, 2018 WL 1569727, at *3 (N.D. Cal. Mar. 30, 2018) (defendant deliberately altered Skype conversation and denied that the native form of the conversation existed; Court awarded an adverse inference instruction at trial and reimbursement to GoPro of the costs incurred in retaining expert that demonstrated metadata had been altered).

Many courts are still looking to establish prejudice before deciding whether intent to deprive was met.⁵⁰ As indicated in the 2015 advisory committee notes, this approach is incorrect:

47. Auer v. City of Minot, 896 F.3d 854, 858 (8th Cir. 2018) ("Auer did not present sufficient evidence of this serious and specific sort of culpability. She supported her request with allegations that incriminating voice mails, e-mails, and other electronic communications were lost because the city failed to properly search some computers, tablets, and phones; waited too long to search others; and generally failed to take basic steps necessary to find and preserve files that could be relevant to her case. Still, her allegations would at most prove negligence in the city's handling of electronic information, not the sort of intentional, bad-faith misconduct required to grant an adverse presumption.").

48. Lokai Holdings LLC v. Twin Tiger USA LLC, No. 15CV9363 (ALC) (DF), 2018 WL 1512055, at *8 (S.D.N.Y. Mar. 12, 2018).

^{46.} Moody v. CSX Transportation, Inc., 271 F. Supp. 3d 410, 432 (W.D.N.Y. 2017) "([E]ven accepting as credible defendants' explanation for the loss of the event recorder data, this Court still concludes that defendants' actions presented sufficient circumstantial evidence from which to infer that they intended to deprive Moody of the relevant data."). See Ottoson v. SMBC Leasing & Fin., Inc., No. 13 Civ. 152, 2017 WL 2992726, at *9 (S.D.N.Y. 2017) ("Intentional failure to take steps necessary to preserve relevant evidence 'satisfies the requisite level of intent required by Federal Rule of Civil Procedure 37(e).' Here, even if Lewandowski's initial error in uploading the event recorder data to the Vault is excused, defendants' repeated failure over a period of years to confirm that the data had been properly preserved despite its ongoing and affirmative rule 11 and rule 26 obligations, particularly before discarding Lewandowski's laptop, is so stunningly derelict as to evince intentionality."); Goldrich v. City of Jersev City, No. CV15885SDWLDW, 2018 WL 4489674, at *2 (D.N.J. Sept. 19, 2018) (circumstantial evidence of bad faith and intent; "Contrary to Plaintiff's representations that he had transferred evidence from the laptop to two USB devices, [the forensic expert] 'determined that these drives had never interfaced with the [1]aptop' and that none of the files on the USB drives 'were ever located on the [1]aptop.' Moreover, despite Plaintiff's assertions that the laptop had been infected with a virus, [the forensic expert] testified that there was never a virus on the laptop. Plaintiff has not presented anything to rebut the evidence before this Court."); Alabama Aircraft Indus., Inc. v. Boeing Co., 319 F.R.D. 730, 746 (N.D. Ala. 2017), motion to certify appeal denied, No. 2:11-CV-03577-RDP, 2017 WL 4572484 (N.D. Ala. Apr. 3, 2017) ("[T]here is no direct evidence of an intent to deprive Pemco of Blake's ESI in this litigation. But there certainly is sufficient circumstantial evidence for the court to conclude that Boeing's agents acted with an intent to delete (or destroy) ESI on Blake's computer in order to hide from Pemco what Blake possessed at a time when Boeing should have anticipated litigation related to the terminated MOA and/or for a jury to infer that Boeing wished to conceal what information was on Blake's computer. As discussed above, Boeing anticipated (or, at a minimum should have anticipated) litigation with Pemco, and the parties had agreed to a manner of handling Pemco-related ESI. In furtherance of that agreement, Boeing instituted a Firewall Plan calling for Pemco-related ESI to be removed from Boeing employees' computers and sent to the legal department. Blake's Pemco-related ESI was intentionally destroyed by an affirmative act which has not been credibly explained. Smith and Holden knew how to comply with the Firewall Plan (and they did so with their own information), but failed to do so with Blake's. No credible explanation has been given as to why they departed from the Firewall Plan's protocols and intentionally deleted Blake's information."); BankDirect Capital Fin., LLC v. Capital Premium Fin., Inc., No. 15 C 10340, 2018 WL 1616725, at *11 (N.D. Ill. Apr. 4, 2018) ("Here, there is no 'direct' evidence of intent-at least in the sense the term is most often used. But there almost never is, and, in any event, direct evidence is not needed. Circumstantial evidence will suffice."); Basra v. Ecklund Logistics, Inc., No. 8:16CV83, 2017 WL 1207482 (D. Neb. Mar. 31, 2017) (Accident logs and reports were destroyed. Court found that recordkeeping was less than meticulous but did not meet intent to suppress the truth. Rule 37 not mentioned specifically.).

Subdivision (e)(2) does not include a requirement that the court find prejudice to the party deprived of the information. This is because the finding of intent required by the subdivision can support not only an inference that the lost information was unfavorable to the party that intentionally destroyed it, but also an inference that the opposing party was prejudiced by the loss of information that would have favored its position.

One case has concluded that although the party destroyed documents intentionally, the destruction was not done in bad faith. The spoliator argued that he destroyed the documents to prevent an overseas competitor from obtaining his purported trade secrets. *Simone v. VSL Pharm., Inc.*, No. CV TDC-15-1356, 2018 WL 1365848, at *4 (D. Md. Mar. 16, 2018).⁵¹ This case raises but did not address a unique kink in rule 37(e). The rule provides that "only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation" may the court impose rule 37(e)(2) sanctions. The Court in Simone decided the case without reference to rule 37 and awarded only reasonable costs and attorney's fees associated with De Simone's spoliation.

50. See, e.g., Zamora v. Stellar Mgmt. Grp., Inc., No. 3:16-05028-CV-RK, 2017 WL 1362688, at *2 (W.D. Mo. Apr. 11, 2017).

51. See also Mueller v. Swift, No. 15-CV-1974-WJM-KLM, 2017 WL 3058027, at *6 (D. Colo. July 19, 2017) (concluding no intent to deprive even though "Plaintiff had numerous opportunities to take easy steps to prevent this ultimate loss of evidence, but failed to do so." "He made the decision—inexplicably, in the Court's view—to alter the original evidence and to present his lawyer with only 'clips' hand-picked from the underlying evidence. This reflects that he obviously intended to make use of portions of the recording to advance his own claims. Plaintiff nevertheless failed to take any number of rather obvious steps to assure that this evidence was not lost. While the spill of liquid on his laptop may not have been Plaintiff's fault, it was an entirely foreseeable risk. Indeed, the same thing had happened to Plaintiff's previous laptop not long before. Plaintiff could and should have made sure that some means of backing up the files relevant to litigation was in place, but this was not done." Court declined to give an adverse jury instruction but would allow the defendants to cross examine plaintiff in front of the jury regarding the spoliation.).

^{49.} See, e.g., Eaton-Stephens v. Grapevine Colleyville Indep. Sch. Dist., 715 F. App'x 351, 354 (5th Cir. 2017) (note this case did not interpret rule 37, but nevertheless may be informative) ("Eaton-Stephens also argues she should have received a spoliation inference [assisting her opposition to defendant's motion for summary judgment] because her computer's contents were erased, and that, because the School District's policy and rules required retention of the contents for several years, the only conclusion was that the action was taken in bad faith. Our cases indicate a violation of a rule or regulation pertaining to document retention is not per se bad faith and Eaton-Stephens cites no authority in support of such a per se bad faith where the only evidence she put forth in support of her claim of bad faith was the alleged violation of School District policy and rules."); Alston v. Park Pleasant, Inc., 679 F. App'x 169, 173 (3d Cir. 2017); Rife v. Oklahoma Dep't of Pub. Safety, 854 F.3d 637, 654 (10th Cir.), cert. denied sub nom. Dale v. Rife, 138 S. Ct. 364 (2017); Washington v. Wal-Mart Louisiana LLC, No. CV 16-1403, 2018 WL 2292762, at *5 (W.D. La. May 17, 2018); Wright v. Nat'l Interstate Ins. Co., No. CV 16-16214, 2017 WL 4011206, at *2 (E.D. La. Sept. 12, 2017).

§ 15.3 Texas State Courts

§ 15.3:1 No Texas Rule

As of the publication of this book, the Texas Supreme Court has not yet adopted a Texas rule of civil procedure that addresses spoliation or loss of ESI. The Texas Supreme Court's advisory committee (SCAC) has been studying and developing a rule for the Court's consideration. A copy of the latest proposed rule has been attached as Appendix C to this book. Until such time as the Court formally adopts a rule of civil procedure, the spoliation or loss of ESI is governed by the Court's opinion in *Brookshire Bros. v. Aldridge*, 438 S.W.3d 9 (Tex. 2014).

§ 15.3:2 Brookshire Bros. v. Aldridge

In *Brookshire Bros.*, Aldridge slipped and fell near a Grab-N-Go rotisserie chicken table. About an hour and a half after leaving the store, Aldridge went to the emergency room because of pain. A week later he returned to the store and reported his injuries. A store manager prepared an incident report based on Aldridge's statements and the recollections of the assistant manager who was on duty at the time of Aldridge's fall. The incident report stated that "Aldridge slipped on grease that had leaked out of a container by the 'Grab N Go.'" *Brookshire Bros. v. Aldridge*, 438 S.W.3d 9, 15 (Tex. 2014).

Aldridge's fall was captured by a surveillance camera. After Aldridge reported his injuries, the store's Vice President of Risk Management decided to retain and copy approximately eight minutes of the video, starting just before Aldridge entered the store and concluding shortly after his fall.

Two weeks after his fall Aldridge learned of the video footage and asked the claims department for a copy. The store refused his request but began paying Aldridge's medical expenses. Almost eleven months later, the grocery store stopped paying the medical expenses and notified Aldridge that it had reviewed the video and determined that it was going to deny responsibility. Aldridge then secured an attorney, who requested two and a half hours of video footage from the store cameras. Brookshire Brothers was unable to comply with that request because the footage had been recorded over almost a year earlier. Aldridge then sued under a premises-liability theory. Aldridge argued in the trial court that Brookshire Brothers' failure to preserve additional video footage amounted to spoliation of evidence that would have been helpful to the key issue of whether the spill was on the floor long enough to give

Spoliation and Sanctions

Brookshire Brothers a reasonable opportunity to discover it. Aldridge accordingly moved for a spoliation jury instruction. The trial court granted the instruction and the court of appeals affirmed.

The Texas Supreme Court reversed and announced a new two-step judicial process when assessing sanctions: first, "the trial court must determine, as a question of law, whether a party spoliated evidence"; second, "if spoliation occurred, the court must assess an appropriate remedy." *Brookshire Bros.*, 438 S.W.3d at 14.

In order to determine if a party spoliated evidence, the trial court must find that:

(1) The spoliating party had a duty to reasonably preserve evidence, and (2) the party intentionally or negligently breached that duty by failing to do so. Spoliation findings—and their related sanctions—are to be determined by the trial judge, outside the presence of the jury, in order to avoid unfairly prejudicing the jury by the presentation of evidence that is unrelated to the facts underlying the lawsuit. Accordingly, evidence bearing directly upon whether a party has spoliated evidence is not to be presented to the jury except insofar as it relates to the substance of the lawsuit.

Brookshire Bros., 438 S.W.3d at 14.

§ 15.3:3 When Is Duty to Preserve Triggered?

The duty to preserve evidence "arises only when a party knows or reasonably should know that there is a substantial chance that a claim will be filed and that evidence in its possession or control will be material and relevant to that claim." *Brookshire Bros. v. Aldridge*, 438 S.W.3d 9, 20 (Tex. 2014) (quoting *Wal-Mart Stores v. Johnson*, 106 S.W.3d 718, 722 (Tex. 2003)). Citing *National Tank Co. v. Brotherton*, 851 S.W.2d 193 (Tex. 1993), a case that addressed when a substantial chance of litigation triggered the invocation of work-product privilege, the Brookshire Bros. court stated that a "substantial chance of litigation" meant that "litigation is more than merely an abstract possibility or unwarranted fear." *Brookshire Bros.*, 438 S.W.3d at 20 (citing *Nat'l Tank*, 851 S.W.2d at 204).

§ 15.3:4 Scope of Duty to Preserve

Once a duty to preserve is triggered, a party must determine what must be preserved and the scope of the evidence to be preserved. In Texas state courts[a] party that is on notice of either potential or pending litigation has an obligation to preserve evidence that is relevant to the litigation. "While a litigant is under no duty to keep or retain every document in its possession ... it is under a duty to preserve what it knows, or reasonably should know is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, [or] is the subject of a pending discovery sanction."

Trevino v. Ortega, 969 S.W.2d 950, 957 (Tex. 1998) (citing *Wm. T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984).

Before sanctions can be sought the lost evidence must be material and relevant. In *Brookshire Bros.*, the court recognized "that the party seeking a remedy for spoliation must demonstrate that the other party breached its duty to preserve material and relevant evidence." *Brookshire Bros. v. Aldridge*, 438 S.W.3d 9, 20 (Tex. 2014).

§ 15.3:5 Level of Culpability Required for Spoliation Instruction— Intent to Conceal or Destroy

Despite the Texas Supreme Court's previous endorsement of jury spoliation instructions and its previous statements that existing "remedies, sanctions, and procedures for evidence spoliation are available under Texas jurisprudence" (*Trevino v. Ortega*, 969 S.W.2d 950, 953 (Tex. 1998)) and that trial judges have broad discretion, the *Brookshire Bros.* court concluded "that a party must intentionally spoliate evidence in order for a spoliation instruction to constitute an appropriate remedy." *Brookshire Bros. v. Aldridge*, 438 S.W.3d 9, 23 (Tex. 2014).

According to the Court, intentional spoliation requires intent to conceal or destroy discoverable evidence. *Brookshire Bros.*, 438 S.W.3d at 23–24. Not even a permissive jury instruction may be given for negligent conduct. The court found that "[t]o allow such a severe sanction [such as a permissive adverse inference instruction] as a matter of course when a party has only negligently destroyed evidence is neither just nor proportionate." *Brookshire Bros.*, 438 S.W.3d at 24.

§ 15.3:6 "Willful Blindness"

The *Brookshire Bros.* court included in its definition of intentional spoliation the concept of "willful blindness," which covers the scenario where "a party does not directly destroy evidence known to be relevant and discoverable, but nonetheless 'allows for its destruction." *Brookshire Bros. v. Aldridge*, 438 S.W.3d 9, 24 (Tex. 2014). Indeed, the court specifically recognized that "[t]he issue of willful blindness is especially acute in the context of automatic electronic deletion systems. A party with control over one of these systems who intentionally allows relevant information to be erased can hardly be said to have only negligently destroyed evidence." *Brookshire Bros.*, 438 S.W.3d at 24 n.17.

§ 15.3:7 Reckless Conduct

The court's use of the phrases "willful" and "willfully blind" is problematic. In *Safeco Insurance Co. of America v. Burr*, 551 U.S. 47, 57 (2007), the United States Supreme Court, addressing the term "willful" in the context of the Fair Credit Reporting Act, noted "'willfully' is a 'word of many meanings whose construction is often dependent on the context in which it appears." In *Safeco*, the United States Supreme Court applied the common-law civil liability meaning of willful, observing: "where willfulness is a statutory condition of civil liability, we have generally taken it to cover not only knowing violations of a standard, but reckless ones as well." *Safeco Ins. Co.*, 551 U.S. at 57. Given the Texas Supreme Court's emphasis on a party's intentional spoliation of evidence, it is very unlikely that the court meant to include reckless conduct as well, but that is an open question.

§ 15.3:8 Prejudice Is Apparently Required before the Imposition of Any Sanction—What Constitutes Prejudice?

Although the Court cites to Justice Baker's analysis in *Trevino* on a number of occasions, *Brookshire Bros. v. Aldridge*, 438 S.W.3d 9 (Tex. 2014) is a departure from Justice Baker's concurring opinion. He evaluated prejudice by looking at three factors:

(1) the relevance of the spoliated evidence to key issues in the case; (2) the harmful effect of the evidence on the spoliating party's case or whether the evidence "would have been helpful to the nonspoliating party's case"; and
(3) whether the spoliated evidence "was cumulative of other competent evidence that" may be used instead of the spoliated evidence.

Trevino v. Ortega, 969 S.W.2d 950, 958 (Tex. 1998) (Baker, J., concurring). Given the Texas Supreme Court's conclusion as a matter of law that Aldridge was not prejudiced by the loss of the additional video, what constitutes prejudice is very unclear.

§ 15.3:9 Assuming Prejudice Has Been Established, What Sanctions Can Be Imposed for the Negligent Loss of Evidence?

According to the Court, "rule 215.2 of the Texas Rules of Civil Procedure enumerates a wide array of remedies available to a trial court in addressing discovery abuse, such as an award of attorney's fees or costs to the harmed party, exclusion of evidence, striking a party's pleadings, or even dismissing a party's claims. These remedies are available in the spoliation context. The trial court also has discretion to craft other remedies it deems appropriate in light of the particular facts of an individual case, including the submission of a spoliation instruction to the jury." *Brookshire Bros. v. Aldridge*, 438 S.W.3d 9, 21 (Tex. 2014) (citations omitted).

It is apparent, however, given the language in other parts of the opinion that the striking of a party's pleadings, dismissal of the case, and the submission of a spoliation instruction are not available remedies for the mere negligent loss of evidence.

According to the Texas Supreme Court, a direct relationship must exist between the offensive conduct, the offender, and the sanction imposed. To meet this requirement, a sanction must be directed against the wrongful conduct and toward remedying the prejudice suffered by the innocent party. Second, a sanction must not be excessive, which means it should be no more severe than necessary to satisfy its legitimate purpose. This prong requires the trial court to consider the availability of lesser sanctions and, "in all but the most exceptional cases, actually test the lesser sanctions." *Petroleum Solutions, Inc. v. Head*, 454 S.W.3d 482, 489 (Tex. 2014) ("While the trial court's discretion to remedy an act of spoliation is broad, it is not limitless.").

§ 15.3:10 When Can Spoliation-Related Evidence Be Heard by Jury?

The Texas Supreme Court's restriction on the admission of evidence regarding spoliation is a surprising departure from existing law. Because the trial court determines whether spoliation occurred and the remedy, the court holds that evidence bearing solely on whether a party spoliated evidence or the degree of culpability is irrelevant to the merits of the case and should not be admitted. *Brookshire Bros. v. Aldridge*, 438 S.W.3d 9, 28 (Tex. 2014). The necessity of this departure is explained by the court because of the tendency of spoliation evidence to skew the focus of the trial from the merits to the conduct of the spoliated evidence that is relevant to a claim or defense would be admissible. This evidence would be absolutely critical in assisting the jury in understanding the nature of the spoliated evidence and the inference to be drawn

§ 15.3

Spoliation and Sanctions

from its destruction. But the Texas Supreme Court is clear that evidence unrelated to the merits of the case that "serves only to highlight the spoliating party's breach and culpability" should not be heard by the jury. *Brookshire Bros.*, 438 S.W.3d at 26.

The *Brookshire Brothers* court appears to acknowledge that evidence regarding what the missing video would have shown, including testimony about the cleanup, is admissible. Likewise, some testimony regarding the creation of the video was appropriate as background. But testimony relevant to whether Brookshire Brothers intentionally breached its duty to preserve evidence was improperly admitted. According to the court, substantial focus at trial was on the spoliation in this case and accusations that Brookshire Brothers hid evidence and acted deceptively. Unfortunately, many questions will arise over the parameters of the evidence that should be admitted.

§ 15.3:11 Post-Brookshire Brothers Cases—Sanctions

Denial of Sanctions: In requesting sanctions, it is generally the plaintiff seeking relief for data that has been lost. The Texas Supreme Court has been concerned that these pretrial and trial activities have needlessly turned the attention from the merits of a case to a "gotcha" for the loss of ronmaterial data. However, defendants have not been immune from seeking sanctions measures without justification. *See Nat'l Sec. Fire & Cas. Co. v. Lampson*, No. 09-15-00299-CV, 2016 WL 7018302, at *11 (Tex. App.—Beaumont Dec. 1, 2016, no pet.) ("The record reflects that Lampson filed a claim with National for his damages from Hurricane Ike on September 29, 2008, applied for assistance from SETRPC on March 5, 2010, filed suit against National cn September 3, 2010, and SETRPC demolished the home in May of 2012. Nothing in the record before us suggests that Lampson intentionally spoliated any evidence by allowing SETRPC to demolish the house, nor does the record suggest that the alleged spoliation deprived National of any meaningful ability to present a claim or defense; rather, the record reflects that National vigorously defended itself, and that National had inspected and photographed the home in 2007 during the underwriting process.").

Since the Texas Supreme Court's decisions in *Brookshire Bros.*, *Petroleum v. Head*, and *Wackenhut Corp. v. Gutierrez*, the lower courts of appeals have almost always reversed a trial court's decision to charge a jury with a spoliation instruction. *See Brookshire Bros. v. Aldridge*, 438 S.W.3d 9 (Tex. 2014); *Petroleum Solutions, Inc. v. Head*, 454 S.W.3d 482, 490 (Tex. 2014) ("[T]he trial court abused its discretion in charging the jury with a spoliation instruction and striking Petroleum Solutions' affirmative defenses because those sanctions do not comply with the procedural and substantive standards set forth in *Brookshire Brothers*. The harm of such sanctions, which

foreclose (or at least severely impede) a party from presenting the merits of its claims or defenses, is typically patent and is compounded by improper presentation of evidence and argument to the jury on the spoliation issue."); Wackenhut Corp. v. Gutierrez, 453 S.W.3d 917, 921 (Tex. 2015) ("To justify the [adverse inference jury] instruction based on this negligence finding, the spoliation must have irreparably deprived Gutierrez of any meaningful ability to present his claims. Thus, we conclude, Wackenhut's failure to preserve the recording did not do. The evidence presented at trial included: the testimony of both drivers; the testimony of an eyewitness Wackenhut employee; witness statements prepared by the drivers and the witness at the time of the accident; testimony of the responding police officer; the police report; Wackenhut's report to its corporate headquarters; photos of the vehicles and the accident scene; and extensive medical records. In light of the abundance of available evidence, we hold that Gutierrez was not irreparably deprived of any meaningful ability to present his claim. Therefore, the trial court abused its discretion by submitting the spoliation instruction to the jury."); Flagstar Bank, FSB v. Walker, 451 S.W.3d 490, 507 (Tex. App.—Dallas 2014, no pet.) ("There is nothing to indicate the missing evidence of these other transactions would not have been cumulative. More important, there is nothing to establish or even suggest that the lack of such evidence deprived Flagstar of a meaningful opportunity to present its case."); IQ Holdings, Inc. v. Stewart Title Guar. Co., 451 S.W.3d 861, 869 (Tex. App.-Houston [1st Dist.] 2014, no pet.) ("IQ also contends that STGC and STC may have destroyed other documents unavailable to it because STC destroyed the hard-copy file. Lester, however, testified that, to the best of his knowledge, all the documents pertaining to the 2006 transaction were preserved in the SureClose system. The trial court could have credited this testimony, believed that STC had electronically stored the closing file, and thus reasonably could have determined that STGC and STC did not breach their duty to preserve. Accordingly, we hold that the trial court acted within its discretion in denying IQ's motion for sanctions."); Nat'l Lloyds Ins. Co. v. Lewis, No. 09-13-00413-CV, 2015 WL 690807, at *11 (Tex. App.-Beaumont Feb. 19, 2015, pet. denied) ("Nothing in the record suggests that Lewis intentionally selected the demolition date in an attempt at spoliation, nor does the record suggest that the alleged spoliation irreparably deprived Lloyds of any meaningful ability to present a claim or defense; rather, the record reflects that Lloyds vigorously defended itself. We conclude that the trial court did not err by refusing to submit Lloyds's requested spoliation instruction."); Pilgrim's Pride Corp. v. Mansfield, No. 09-13-00518-CV, 2015 WL 794908, at *7 (Tex. App.—Beaumont Feb. 26, 2015) supplemented by No. 09-13-00518-CV, 2015 WL 994643 (Tex. App.—Beaumont Mar. 5, 2015) ("Pilgrim's argues that the severity of the accident was sufficient to place the grocer on notice that Judy would pursue a claim. However, the record reflects that after Judy fell, she declined Williamson's

Spoliation and Sanctions

suggestion that she get medical attention because she did not think she needed any treatment at that time. The testimony further reflects that Judy left the store without stating that she intended to sue or file a claim. Given the lack of evidence to indicate the grocer was on notice that Judy would later seek to recover for the injuries she suffered that day, the trial court's conclusion is reasonable, as it is based on the testimony showing the grocer was not on notice on the day Judy fell that she would subsequently seek to recover for the injuries she suffered that day. We conclude the trial court did not abuse its discretion by refusing Pilgrim's requested instruction on its spoliation claim."); Smith v. Williams, No. 06-14-00040-CV, 2015 WL 3526089, at *8-9 (Tex. App.-Texarkana May 29, 2015, no pet.) ("[T]here is no evidence that these logs were destroyed because of their evidentiary value or that Medallion Transport allowed their destruction 'in a purposeful effort to conceal relevant evidence.' Since the evidence required to find intentional spoliation is lacking, we find that giving the spoliation instruction ran afoul of Brookshire Bros. Having found an abuse of discretion in giving the spoliation instruction, we may reverse the judgment on this basis only if giving the instruction 'probably caused the rendition of an improper judgment."" (internal citations omitted)); DeLeon v. Lacey, No. 03-13-00292-CV, 2015 WL 4449436, at *4 (Tex. App.-Austin July 15, 2015, no pet.) ("Lacey had firsthand knowledge of the roof, having built it; Lacey had eight or nine opportunities to inspect the roof in the eighteen months before Bickel repaired it; Lacey made no requests in the course of formal discovery, or otherwise, to inspect the roof after he told DeLeon that the warranty period had expired; Lacey testified that he installed a 'base sheet up the transition to the steep slope side' of the DeLeon roof and sealed it-i.e., he was able to contradict Pritchard's testimory regarding the construction; Lacey's focus at trial was on the other possible causes of leaks and his evidence that he installed the roof in a good and workmanlike manner; Lacey presented an expert witness who was able to testify on Lacey's behalf; and Lacey did not challenge Pritchard's testimony regarding the installation. Taking all these matters into consideration, as the district court would have had to do, we cannot say that the district court abused its discretion in refusing to exclude all evidence regarding the cause of the roof's leak, even if we assume spoliation by DeLeon."); In re A.H.J., No. 05-15-00501-CV, 2015 WL 5866256, at *8 (Tex. App.-Dallas Oct. 8, 2015, pet. denied) ("Although the Department video recorded over forty visits appellant had with her children, the Department preserved and produced only five of the video recordings in response to appellant's discovery requests Here, there was no proof that the Department acted with the specific intent to conceal evidence or, if the Department acted negligently, the spoliation irreparably deprived appellant of any meaningful ability to present her defensive theory that she could parent her children."); Shamoun & Norman, LLP v. Hill, 483 S.W. 3d 767, 793 (Tex. App.-Dallas 2017, aff'd in part and rev'd in part on other

grounds, 544 S.W. 3d 724 (Tex. 2018) ("Even assuming S & N had a duty to preserve evidence, the record supports a finding that the trial court could have determined S & N did not intentionally destroy evidence. S & N presented evidence that a 'computer glitch' with its servers resulted in only Shamoun's e-mails being destroyed. Shamoun willingly admitted some e-mails were lost but said the inadvertent loss was beyond his control. The loss occurred while a third party performed server updates. An e-mail sent on May 12, 2010, from Greg Moore to Shamoun explained the unexpected corruption of the old server and said, 'As of right now, expect that all of your e-mail that has not been moved into iManage (Doc Management) is gone and not recoverable.").

In *Knoderer v. State Farm Lloyds*, 515 S.W.3d 21, 38 (Tex. App.—Texarkana 2017, pet. denied), a party fabricated evidence, which he then used in the proceeding, and, after evidence surfaced indicating he fabricated the evidence, destroyed the only evidence that would conclusively establish his fabrication. The appellate court concluded that the trial court improperly allowed spoliation evidence in trial but found harmless error.

Limited Sanctions Awarded: Texas court of appeals decisions affirming sanctions in excess of an attorney's fees sanction are few. *See Telesis/Parkwood Ret. I, Ltd. v. Anderson*, 462 S.W.3d 212, 255 (Tex. App.—El Paso 2015, no pet.) ("Edna alleged that she was unable to get up and repeatedly pulled the cord on her apartment's emergency call system. Because no one from Parkwood responded to her calls and no one inquired about Edna's whereabouts or condition when she failed to appear for her daily midday meal at Parkwood on July 6, 2008, Edna remained on the floor of her apartment, naked, without food or water, and eventually in her own waste . . . Edna was [eventually] hospitalized with injuries and diagnosed with rhabdomyolysis, a condition alleged to have resulted from these events . . . The evidence shows and supports the trial court's conclusion that Telesis knew or reasonably should have known that there was a substantial chance that Edna would file a claim, and that the emergency call unit, specifically the transmitter from Edna's room that was replaced before she was transported from her apartment to the hospital and was then thrown away by Nafziger, would be material and relevant to that claim.").

A case where sanctions were upheld is *In re Advanced Powder Solutions, Inc.*, 496 S.W.3d 838 (Tex. App.—Houston [1st Dist.] 2016, no pet.). In that case the employee was injured in an explosion. The event was captured on a video system:

Before the security camera system recorded over the video, [the employer] used the video to determine "exactly what happened that day." In August 2015, nearly two years after the accident, Baker used this knowledge to

plan, conduct, and film an "experiment . . . to recreate the accident" by "repeating the steps that happened that day," specifically by testing what happened if someone was "loading powder [into the reactor involved in the incident] . . . the way we normally do it and someone had done what Donnie Guzman had done" in opening a valve.

In re Advanced Powder Solutions, Inc., 496 S.W. 3d at 844.

The Court concluded that the employer had a duty to preserve the video, failed to do so, and the employee was prejudiced by the spoliation. The appellate court reversed the striking of pleadings but affirmed the trial court's issuance of a spoliation instruction.

In *In re Beck*, No. 13-19-00174-CV, 2019 WL 1856620, at *1 (Tex. App.—Corpus Christi–Edinburg Apr. 25, 2019, mandamus pending), the relator argued that the trial court abused its discretion by granting a motion for sanctions filed by the executor of the estate of Douglas H. Beck. The trial court found that the relator had a duty to preserve the evidence of certain blood samples, that he breached that duty, and that the real party was harmed and prejudiced thereby. The trial court prohibited the relator from using the autopsy results, and the report and deposition of Dr. Adel Shaker to the extent they relied on the blood samples. The court of appeals rejected the argument that this was a death penalty sanction and denied the mandamus petition.

In *In re J.H. Walker, Inc.*, No. 05-14-01497-CV, 2016 WL 819592, at *11 (Tex. App.—Dallas Jan. 15, 2016, no pet.), the court found that a nonsubscriber employer intentionally spoliated evidence when it failed to preserve a truck involved in a fatality. Nevertheless, the court of appeals remanded for consideration of lesser sanctions because the trial court abused its discretion by striking Walker Trucking's workers' compensation defense and its pleadings, essentially adjudicating the dispute.

In *Bellow v. Bellow*, No. 09-16-00252-CV, 2018 WL 2974477, at *5 (Tex. App.— Beaumont June 14, 2018, pet. denied), the trial court expressly ordered David to provide cellular telephones for downloading and inspection as there were allegations the videos produced had been edited. The cellphones produced by David for forensic examination did not contain the videos, and at least one of the cellphones had been wiped clean of all data. Sanctions of \$3,000 in this divorce case were imposed and affirmed by the appellate court.

In *Hogg v. Lynch, Chappell & Alsup, P.C.*, 553 S.W.3d 55, 68 (Tex. App.—El Paso 2018, no pet.), an attorney-client dispute, Hogg sent an e-mail in which she admitted

to having recordings between her and her former attorneys. The appellate court concluded that this was a party admission. The appellate court affirmed the trial court's order excluding evidence of her conversations with her attorneys as proportional.

In *Scarbrough v. Purser*, No. 03-13-00025-CV, 2016 WL 7583546, at *20 (Tex. App.—Austin Dec. 30, 2016, pet. denied), an attorney who was a party in the case was sanctioned for "his intentional concealment and deception regarding the existence of audio recordings."

For a case taking a more relaxed interpretation of *Brookshire Bros.*, see *Mercedes-Benz USA*, *LLC v. Carduco*, *Inc.*, No. 13-13-00296-CV, 2016 WL 1274535, at *25 (Tex. App.—Corpus Christi–Edinburg Mar. 31, 2016, *rev'd on other grounds*, No. 16-0644, 2019 WL 847845 (Tex. Feb. 22, 2019) (sufficient evidence existed either that MBUSA destroyed relevant evidence, and MBUSA failed to establish that the evidence was cumulative of other evidence in the record).

§ 15.4 Conclusion

The ability to recover sanctions for the loss or spoliation of evidence has significantly changed with the adoption of Federal Rule of Civil Procedure 26(e) and the Texas Supreme Court's opinion in *Brookshire Bros. v. Aldridge*, 438 S.W.3d 9 (Tex. 2014). According to various sources, sanctions have dropped after the 2015 amendment to Federal Rules of Civil Procedure rule 37(e). The same trend appears to have occurred in Texas state courts. Nevertheless, some lawyers note they are still under pressure to collect and preserve data from rapidly advancing technology. Although parties are not obliged to preserve everything and proportionality analyses need to be applied, it is difficult to criticize litigants for seeking sanctions when they may bear the burden of proof on an issue. Nevertheless, requesting parties must ensure that they have established all elements under either Fed. R. Civ. P. 37(e) or *Brookshire Bros.* prior to the filing of any motion for sanctions. Parties resisting any such relief should be prepared to address why any relevant, proportional data has been lost and why either prejudice or intentional spoliation has not occurred.

Chapter 16

Rule 30(b)(6) Depositions

Julia W. Mann, Matthew J. Swantner, and Stephen A. Calhoun

§ 16.1 Introduction

The continuing proliferation of electronically stored information ("ESI") has not only had a profound impact on the volume of discovery, it has also changed the type of information litigants seek about the discovery process itself. E-discovery has resulted in a new layer of discovery focused not on the merits of a dispute, but instead on an organization's data-storage systems and its compliance with duties to preserve, collect, review, and produce relevant documents. This type of non-merits discovery is often referred to as discovery on discovery, discovery about discovery, "meta-discovery,"1 or, as labeled by one recent commentator, "process-directed discovery."2 One of the most common methods for pursuing process-directed discovery is a deposition under Federal Rule of Civil Procedure 30(b)(6) or its Texas state law counterpart, Texas Rule of Civil Procedure 199.2(b)(1). These rules enable a party to depose an organization involved in the litigation rather than attempting to determine the single individual who may have the most know edge of the organization's data. For the pupose of this chapter, a deposition under Federal Rule of Civil Procedure 30(b)(6) or Texas Rule of Civil Procedure 199.2(b)(1) will be referred to as a "corporate deposition."

Process-directed corporate depositions typically focus on two broad categories of issues: data-storage issues (e.g., details of the party's IT systems, custodians, and data) and discovery-process issues (e.g., the party's efforts to preserve, collect, review, and produce relevant ESI). Failure to properly preserve, collect, and produce ESI can result in a broad array of sanctions; thus, when a company is faced with an e-discovery corporate deposition, properly selecting and preparing a representative or

^{1.} See generally Hon. Xavier Rodriguez and Hon. David L. Horan, *Meta-Discovery: Allegations of an Incomplete Document Production*, 19 Sedona Conf. J. 745 (2018) (hereinafter cited as "Rodriguez and Horan, *Meta Discovery*").

^{2.} Hon. Craig B. Shaffer, *Deconstructing "Discovery about Discovery,"* 19 Sedona Conf. J. 215, 217 (2018) (hereinafter cited as "Schaffer, *Deconstructing "Discovery about Discovery"*) (distinguishing "process-directed discovery") from "merits-directed discovery").

§ 16.1

representatives is paramount.³ In that regard, IT professionals who previously were behind the scenes in the discovery process are becoming key witness as they are asked to testify regarding all aspects of a corporation's records retention policy and data management systems. Given this potential inquiry, it is important for parties to plan for e-discovery corporate depositions from the outset of the litigation so that they are not left scrambling to select and prepare witnesses when depositions are actually noticed.

§ 16.2 Corporate Depositions Generally

§ 16.2:1 Federal Rule of Civil Procedure 30(b)(6)

Federal Rule of Civil Procedure 30(b)(6) is a well-established tool to discover the corporate position of an organization on a variety of matters. The rule requires the party seeking the deposition to first describe "with reasonable particularity" the topics on which it seeks testimony from the organization.⁴ Only after the requesting party has met its burden is the noticed party required to produce one or more witnesses.⁵ Thus, "[t]he requesting party must take care to designate, with painstaking specificity, the particular subject areas that are intended to be questioned, and that are relevant to the issues in dispute."⁶

Once the noticing party meets its burden, the noticed party must designate and present a witness able to testify about information "known or reasonably available to the organization."⁷ Where the organization does not have knowledge on noticed topics, "its obligations under rule 30(b)(6) obviously cease, since the rule requires testimony only as to 'matters known or reasonably available to the organization."⁸ But for topics on which the company does have information, the company has an obligation to educate and prepare its witness, including through review of documents or prior deposition testimony.⁹ The rule 30(b)(6) witness is sometimes described as the "person

^{3.} Chapter 15 discusses spoliation issues and sanctions in detail. Section 16.4 of this chapter addresses sanctions in the context of e-discovery corporate depositions.

^{4.} Fed. R. Civ. P. 30(b)(6).

^{5.} Dwelly v. Yamaha Motor Corp., 214 F.R.D. 537, 540 (D. Minn. 2003); Prokosch v. Catalina Lighting, Inc., 193 F.R.D. 633, 638 (D. Minn. 2000); Starlight Int'l Inc. v. Herlihy, 186 F.R.D. 626, 639 (D. Kan. 1999).

^{6.} Prokosch, 193 F.R.D. at 638 (emphasis added).

^{7.} Fed. R. Civ. P. 30(b)(6); Tex. R. Civ. P. 199.2(b).

^{8.} Dravo Corp. v. Liberty Mutual Ins. Co., 164 F.R.D. 70, 76 (D. Neb. 1995) (quoting Fed. R. Civ. P. 30(b)(6)).

§ 16.2

most knowledgeable" about a particular topic, but the rules do not require the individual with the most personal knowledge to be designated.¹⁰ Indeed, the corporate witness will often need to be educated to testify about multiple areas outside of his personal knowledge.

§ 16.2:2 Texas Rule of Civil Procedure 199.2(b)(1)

The Texas rule on corporate depositions are very similar to the federal rule. Under Texas Rule of Civil Procedure 199.2(b)(1), a notice of deposition may name a corporation, partnership, association, governmental agency, or other organization as the witness.¹¹ The notice of deposition must describe "with reasonable particularity the matters on which examination is requested."¹² In response, the noticed organization must, within "a reasonable time before the deposition," designate one or more individuals to testify on its behalf.¹³ In the event more than one individual is designated, the entity must identify the person testifying with respect to each area of inquiry.¹⁴ Each person testifying on behalf of the entity must testify as to matters that are "known or reasonably available to the organization."¹⁵ Thus, just as under the federal rules, the witness does not have to have personal knowledge and may have to be educated about a particular subject.

§ 16.2:3 Effect of Corporate Deposition Testimony

A corporate deposition "is admissible against the party designating the representative but is not 'binding' on the entity for which the witness testifies in the sense of preclusion or judicial admission."¹⁶ The testimony given in a corporate deposition is evidence, which, like other deposition testimony, can be used for impeachment purposes if it is later contradicted by the corporation.¹⁷ In the event that contrary information

- 13. Tex. R. Civ. P. 199.2(b)(1).
- 14. Tex. R. Civ. P. 199.2(b)(1).
- 15. Tex. R. Civ. P. 199.2(b)(1).

16. Lindquist v. City of Pasadena, Tex., 656 F. Supp. 2d 662, 698 (S.D. Tex. 2009) (citing Charles A. Wright, Arthur R. Miller, and Richard L. Marcus, Federal Practice & Procedure § 2103 (2d ed. 1994)).

^{9.} Prokosch, 193 F.R.D. at 638-39.

^{10.} QBE Ins. Corp. v. Jorda Enters., Inc., 277 F.R.D. 676, 688 (S.D. Fla. 2012).

^{11.} Tex. R. Civ. P. 199.2(b)(1); Allstate Tex. Lloyds v. Johnson, 784 S.W.2d 100, 104 (Tex. App.-Waco 1989, no writ).

^{12.} Tex. R. Civ. P. 199.2(b)(1).

that was known or available at the deposition is later offered at trial, the deposition testimony may be offered to impeach the witness.¹⁸

§ 16.2:4 Use of Corporate Depositions for E-Discovery Issues

While parties have the option of seeking deposition testimony from individual officers, directors, and employees of an entity, corporate depositions are designed "to avoid the possibility that several officers and managing agents might be deposed in turn, with each disclaiming personal knowledge of facts that are clearly known to persons within the organization and thus to the organization itself."¹⁹ Corporate depositions thus obviate the need to issue interrogatories to determine the identity of persons most knowledgeable about the location and preservation of relevant ESI. Moreover, given the limitations on the number of permitted depositions,²⁰ it may be impossible to depose each individual with knowledge of the entity's ESI as well as all relevant fact witnesses. The ability to notice a single deposition²¹ of the entity to obtain testimony related to each phase of the discovery process is a powerful tool when investigating a potential claim for spoliation or other discovery abuses.

§ 16.3 Resisting an E-Discovery Corporate Deposition

Process-directed discovery can add a whole new layer of costs and operational burdens to the already costly and burdensome discovery process. This type of discovery also carries the risk of being used as a pure litigation tactic rather than a legitimate tool for "secur[ing] the just, speedy, and inexpensive determination of every action

20. See Fed. R. Civ. P. 30(a)(2) (requiring leave of court for a party to notice more than ten depositions without agreement from all parties); 30(d)(1) (limiting each deposition to seven hours unless otherwise stipulated by the parties or ordered by the court); Tex. R. Civ. P. 190.2(b)(2), 190.3(b)(2), 190.4(b) (addressing limits on depositions under various discovery control plan levels).

^{17.} A.I. Credit Corp. v. Legion Ins. Co., 265 F.3d 630, 637 (7th Cir. 2001) (citation omitted); see also Diamond Triumph Auto Glass, Inc. v. Safelite Glass Corp., 441 F. Supp. 2d 695, 723 n.17 (M.D. Pa. 2006) (rejecting the plaintiff's argument that the court should limit the defendant to the testimony of its corporate representative simply because "the witness could not answer the questions" even though the plaintiff never filed a motion to compel or a motion for sanctions and because "[t]he Federal Rules of Civil Procedure do not allow such a severe sanction under these circumstances").

^{18.} Crompton Greaves, Ltd. v. Shippers Stevedoring Co., 776 F. Supp. 2d 375, 392 n.11. (S.D. Tex. 2011).

^{19.} Brazos River Auth. v. GE Ionics, Inc., 469 F.3d 416, 432–33 (5th Cir. 2006) (citation omitted); see also Reilly v. Nat'l Markets Grp. Inc., 181 F.3d 253, 268 (2d Cir. 1999) (imposing sanctions including preclusion of evidence for failure to comply with rule 30(b)(6)).

^{21.} Fed. R. Civ. P. 30 advisory committee notes to the 1993 amendments ("A deposition under rule 30(b)(6) should, for purposes of this limit, be treated as a single deposition even though more than one person may be designated to testify.").

and proceeding," as required by Federal Rule of Civil Procedure 1.²² And because process-directed discovery by definition focuses on background issues rather than the substantive merits of the parties' claims and defenses, it raises legitimate questions of relevance, privilege, and—especially since the 2015 amendments to the federal rules—proportionality.

For these reasons, many litigants, commentators, and judges have expressed strong reservations about process-directed discovery and have promoted severe limitations on its use.²³ Yet in some cases, formal discovery into a party's data-storage systems or even its conduct in fulfilling its discovery obligations is appropriate and necessary.²⁴ "[N]o clear standard has emerged" from courts' efforts to balance these interests, although "the consensus view from the federal case law appears to dictate that a party should not be required to provide discovery about its production process without good cause,"²⁵ usually in the form of some evidence of incomplete production or other discovery abuses.

§ 16.3:1 Resisting Discovery on Data-Storage Issues

Of the two broad categories of process-directed discovery topics, data-storage issues are more innocuous than discovery-process issues. After all, pure data-storage issues—for example, a description of the party's IT hardware and software and the organization of its file storage—are much less likely to raise concerns of attorney-client privilege and work product protection. Data-storage issues also fall more squarely within the scope of appropriate discovery defined by the federal rules.²⁶ Before the

24. See, e.g., Sinclair Wyo. Ref. Co. v. A&B Builders, Ltd., No. 15-CV-91-ABJ, 2017 U.S. Dist. LEXIS 222825, at *5 (D. Wyo. Oct. 31, 2017) ("While discovery on discovery is generally improper, the Court finds there is sufficient evidence that raises the issue of spoliation at this time. Further discovery into the issue may show its existence or nonexistence.").

^{22.} Fed. R. Civ. P. 1; see also Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354, 357 (D. Md. 2008); Michael Darren Sparks, Meta-Discovery or Discovery About Discovery: Is it Proper to Discover an Opposing Party's Efforts to Comply with Discovery Requests?, 29 The Company Lawyer Vol. 10 309, 309 (2008) ("In the new era of e-discovery, meta-discovery is a potent weapon rife with problems of privilege, expense and the specter of harassment.").

^{23.} See, e.g., Jensen v. BMW of N. Am., LLC, 328 F.R.D. 557, 566 (S.D. Cal. 2019) ("Discovery into another party's discovery process is disfavored."); Karrani v. JetBlue Airways Corp., No. C18-1510 RSM, 2019 U.S. Dist. LEXIS 89031, at *12 (W.D. Wash. May 28, 2019) ("Such 'meta-discovery' is highly disfavored, and courts may only allow such discovery 'where there is some indication that a party's discovery has been insufficient or deficient."").

^{25.} Rodriguez & Horan, Meta-Discovery, at 763.

^{26.} See Schaffer, *Deconstructing "Discovery about Discovery,"* at 233 ("The Federal Rules of Civil Procedure have long recognized that information about a party's organizational arrangements or filing systems may be discoverable.").

2015 amendments, Fed. R. Civ. P. 26 expressly allowed discovery into "the existence, description, nature, custody, condition, and location of any documents or tangible things."²⁷ This portion of rule 26 was deleted in the 2015 amendments, but the deletion was "more style than substance."²⁸ The advisory committee notes explain that because "[d]iscovery of such matters is so deeply entrenched in practice[,] it is no longer necessary to clutter the long text of rule 26 with these examples."²⁹ The notes do emphasize the revised rule's increased focus on proportionality, however, directing that "discovery identified in these examples should still be permitted under the revised rule *when relevant and proportional to the needs of the case*."³⁰

Proportionality arguments likely provide the most effective means to avoid discovery into data-storage issues, especially when requested at the outset of a lawsuit.³¹ Although the advisory committee notes acknowledge that "detailed information about another party's information systems and other information resources" may be helpful in framing discovery requests,³² the benefit will often be outweighed by the corresponding burden of formal discovery.³³ In *Miller v. York Rise Services Group*—a pre-2015 amendment case—the U.S. District Court for the District of Arizona rejected a party's request for a "rule 30(b)(6) deposition regarding the manner and methods used by Defendant to store and maintain electronically stored information."³⁴ The court observed that "it remains to be determined whether starting the discovery process with a wide ranging inquiry into the manner and method by which a party stores and manages ESI is a helpful and appropriate approach to obtaining substantive information," concluding: "In this court's view it is not."³⁵ The court went on to opine that "starting discovery with such an inquiry puts the cart before the horse and likely will

- 27. Fed. R. Civ. P. 26(b)(1) (2014); see also Tex. R. Civ. P. 192.3(b) ("A party may obtain discovery of the existence, description, nature, custody, condition, location, and contents of documents and tangible things . . . that constitute or contain matters relevant to the subject matter of the action.").
- 28. Immanuel R. Foster, Proportionality Emphasized in Amendments to the Federal Rules of Civil Procedure, 60 B.B.J. 17, 18 (2016).
 - 29. Fed. R. Civ. P. 26(b)(1) advisory committee notes to the 2015 amendments.
 - 30. Fed. R. Civ. P. 26(b)(1) advisory committee notes to the 2015 amendments (emphasis added).

31. See Foster, *Proportionality Emphasized*, at 18 ("[T]he revision [to rule 26(b)(1) in the 2015 amendments] suggests limitations to the scope of this [process-directed] discovery to the extent that it would be at cross purposes with proportionality.").

32. Fed. R. Civ. P. 26(b)(1) advisory committee notes to the 2015 amendments.

33. See Schaffer, Deconstructing "Discovery about Discovery," at 235, 262 ("Pursuing discovery in order to draft discovery seems, at the very least, unnecessarily expensive."); ("In the typical case, . . . early [process-directed] discovery efforts will have little practical value in promoting the goals of rule 1.").

34. No. 2:13-cv-1419 JWS, 2014 U.S. Dist. LEXIS 51859, at *1 (D. Ariz. Apr. 15, 2014).

35. Miller, 2014 U.S. Dist. LEXIS 51859, at *5.
Rule 30(b)(6) Depositions

increase, rather than decrease, discovery disputes," although it acknowledged that such a deposition might become necessary later in the course of the lawsuit.³⁶

Courts and commentators alike have observed that the ideal method for exchanging information on data-storage issues is through informal cooperation of counsel rather than formal discovery from the parties.³⁷ Indeed, the federal rules envision attorneys addressing a variety of e-discovery issues at both the rule 26(f) conference and the rule 16 scheduling conference.³⁸ Only when these informal efforts break down should formal data-source discovery be pursued.³⁹

37. See, e.g., Commins v. NES Rental Holdings, Inc., No. 3:16CV-00608-GNS, 2018 U.S. Dist. LEXIS 107879, at *27–28 (W.D. Ky. June 28, 2018) ("Because the Court has previously determined it is necessary for Plaintiffs and [Defendant] to meet and confer in the next twenty days to reach an agreement as to ESI discovery going forward, including custodians and search terms, it would be inappropriate at this juncture to grant Plaintiffs' request for a [process-directed] rule 30(b)(6) deposition."); Schaffer, *Deconstructing "Discovery about Discovery,"* at 216 (warning that "discovery about discovery' threatens to become a catchphrase in lieu of a reasonable discussion between requesting and producing parties"); Hon. Andrew J. Peck and Hon. John M. Facciola, *E-Discovery: Where We've Been, Where We Are, Where We're Going*, 12 Ave Maria L. Rev. 1, 24–25 (2014) (stating that, "[i]deally, there should not be any formal discovery about discovery" but acknowledging it may be required in cases where "the other side is stonewalling").

38. Fed. R. Civ. P. 26(f); see also Schaffer, Deconstructing "Discovery about Discovery," at 263– 66 (suggesting that the requirement in federal rule 26(b)(2)(C) for courts to limit discovery that can "be obtained from some other source that is more convenient, less burdensome, or less expensive" "plainly implicates the rule 26(f) process" with respect to formal process-related discovery). A standing order issued by Judge Xavier Rodriguez in the Western District of Texas advises parties that "[d]isputes regarding ESI will be resolved more efficiently if, before meeting with opposing counsel, the attorneys for each party review and understand how their client's data is stored and retrieved in order to determine what issues must be addressed during the rule 26 meet and confer conference." See Standing Order in Civil Cases Assigned to Judge Xavier Rodriguez (signed December 1, 2015), Addendum Regarding Discovery, available at: https://coop.txwd.uscourts.gov/wp-content/uploads/Standing%20Orders/ San%20Antonio/Rodriguez/Standing%20Order%20in%20Civil%20Cases%20Assigned%20to% 20Judge%20Xavier%20Rodriguez.pdf.

39. See Watkins v. HireRight, Inc., No. 15CV1432-MMA (BLM), 2013 U.S. Dist. LEXIS 189558, at *8–14 (S.D. Cal. Nov. 18, 2013) (granting protective order for 30(b)(6) topic regarding "how Defendant maintains its computer system," in part because Defendant had already provided extensive information regarding its computer systems through meet-and-confer letters and conferences). Note, however, that objecting to discovery requests on the basis of undue burden may invite data-storage discovery meant to evaluate the actual burdens at issue. See, e.g., Starbucks Corp. v. ADT Sec. Servs., Inc., No. 08-cv-900-JCC, 2009 U.S. Dist. LEXIS 120941 (W.D. Wash. Apr. 30, 2009) (noting that the court had directed a 30(b)(6) deposition of a designated information technology representative in order to analyze objection based on undue burden).

^{36.} *Miller*, 2014 U.S. Dist. LEXIS 51859, at *5; *but cf. Winfield v. City of New York*, No. 15-cv-05236 (LTS) (KHP), 2018 U.S. Dist. LEXIS 22996, at *21–22 (S.D.N.Y. Feb. 12, 2018) (allowing a data-storage 30(b)(6) deposition and expressing "view that, especially with respect to depositions concerning data, it is the joint responsibility of the parties to cooperate so that the corporate entity has a clear understanding of the information sought and can designate the persons most appropriate to testify on those subjects").

§ 16.3:2 Resisting Discovery on Discovery-Process Issues

Requests regarding discovery-process issues—for example, a party's conduct in the case at hand regarding preservation, collection, review, and production of ESI—more directly implicates concerns about relevance⁴⁰ and privilege⁴¹ (in addition to proportionality). These concerns have led many courts to conclude that "[d]iscovery into another party's discovery process is disfavored"⁴² and provide the off-repeated admonition that "[r]equests for such 'meta-discovery' should be closely scrutinized in light of the danger of extending the already costly and time-consuming discovery process ad infinitum."⁴³

As a result, many courts—including state and federal courts in Texas—require a threshold showing of inadequate responses to discovery or other discovery abuses before allowing corporate depositions and other formal discovery regarding discovery-process issues.⁴⁴ The evidentiary standard for this threshold showing, however, is unsettled.⁴⁵ Some courts require a showing of bad faith or intentional misconduct before allowing process-directed discovery.⁴⁶ Other courts do not require bad faith but

41. See, e.g., EEOC v. Boeing Co., No. CV 05-03034-PHX-FJM, 2007 U.S. Dist. LEXIS 29107, at *6-7 (D. Ariz. Apr. 18, 2007) (denying motion to compel 30(b)(6) deposition regarding defendant's efforts to locate requested documents "to the extent that Topic seeks to discovery defense counsel's legal theories regarding the manner in which defendant responded to plaintiff's requests"); In re Exxon Corp., 208 S.W.3d 70, 75 (Tex. App.—Beaumont 2006, orig. proceeding) (concluding that corporate deposition topic "inquiring specifically into the process by which [a party's] representative responded to the requests for production . . . necessarily and almost exclusively concerns the 'mental impressions developed in anticipation of litigation or for trial by or for a party or a party's representatives' and consists of the 'attorney's representative's mental impressions, opinions, conclusions, or legal theories' subject to protection as work product and core work product"); see also generally Sean Grammel, Protecting Search Terms as Opinion Work Product: Applying the Work Product Doctrine to Electronic Discovery, 161 U. Pa. L. Rev. 2063 (2013); Justin Smith, Seeking Discovery of Search Strategies: In re Exxon Corp. and the Work-Product Doctrine in Texas, 63 Baylor L. Rev. 287, 306 note (2011). But see Ferring B.V. v. Fera Pharms., LLC, No. CV 13-4640 (SJF)(AKT), 2016 U.S. Dist. LEXIS 132522, at *8 (E.D.N.Y. Sept. 27, 2016) (directing party to provide its "list of search terms and list of document production topic areas," even if prepared by counsel as part of the litigation, because the requesting party was "entitled to know the methodology and manner of the ESI production undertaken").

42. Jensen v. BMW of N. Am., LLC, 328 F.R.D. 557, 566 (S.D. Cal. 2019).

43. Jensen, 328 F.R.D. at 566 (quoting Freedman v. Weatherford Int'l Ltd., No. 12-cv-2121-LAK-JCF, 2014 WL 4547039, at *2 (S.D.N.Y. Sept. 12, 2014).

^{40.} See, e.g., Fish v. Air & Liquid Sys. Corp., No. GLR-16-496, 2017 WL 697663at *15 (D. Md. Feb. 21, 2017) ("[T]he manner in which [a party] maintains documents for document retention purposes is not relevant to the allegations in this case."); Jackson v. Equifax Info. Servs. LLC, No. 1:13-cv-02382-RLV-RGV, 2014 U.S. Dist. LEXIS 199646, at *9–10 (N.D. Ga. May 21, 2014) (denying motion to compel 30(b)(6) deposition because, other than speculation, requesting party had "not explained 'why [the defendant's] efforts to locate documents are relevant to a claim or defense in this case"); Junk v. Terminix Int'l Co., No. 4:05-cv-00608-REL-RAW, 2008 U.S. Dist. LEXIS 129962, at *9–10 (S.D. Iowa Apr. 10, 2008) ("Discovery concerning discovery has no obvious relevance to the parties' claims or defenses unless there is reason to believe a party has not been forthcoming, which has not been shown.").

still only allow process-directed discovery upon presentation of "concrete evidence" of inadequate responses or discovery abuse.⁴⁷ The Sedona Conference supports this approach, stating that "there should be no discovery on discovery absent . . . specific, tangible, evidence-based indicia (versus general allegations of deficiencies or mere 'speculation') of a material failure by the responding party to meet its obligations."⁴⁸

Under this evidence-focused approach, it is not sufficient to rely on general allegations that the opposing party did not produce as much information as expected.⁴⁹ As one court explained: "Courts supervising discovery are often confronted by the claim that the production made is so paltry that there must be more that has not been pro-

45. See Rodriguez & Horan, Meta-Discovery, at 763-65.

46. Brand Energy & Infrastructure Servs., Inc. v. Irex Corp., No. 16-2499, 2018 U.S. Dist. LEXIS 21810, at *6–7 (E.D. Pa. Feb. 7, 2018) ("Without any showing of bad faith or unlawful withholding of documents . . . requiring such discovery on discovery would unreasonably put the shoe on the other foot and require a producing party to go to herculean and costly lengths ").

47. In re Exxon Corp., 208 S.W.3d 70, 71 (Tex. App.-Beaumont 2006, orig. proceeding).

48. The Sedona Conference, Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 19 Sedona Conf. J. 1, 123 (2018); see also 118 ("Principle 6 recognizes that a responding party is best situated to preserve, search, and produce its own ESI. Principle 6 is grounded in reason, common sense, procedural rules, and common law, and is premised on each party fulfilling its discovery obligations without direction from the court or opposing counsel, and eschewing 'discovery on discovery,' unless specific deficiency is shown in a party's production.").

49. See, e.g., Hubbard v. Potter, 247 F.R.D. 27, 29 (D.D.C. 2008) (rejecting process-directed discovery requested based on "paucity of documents" because court "must have more to go by than a hunch on the plaintiff's part"); Downing v. Abbott Labs., No. 15 CV 5921, 2017 U.S. Dist. LEXIS 181401, at *4–9 (N.D. Ill. Nov. 2, 2017) (rejecting "contention that the 'sparse production of e-mails' from key witnesses and decision makers suggest problems with [the producing party's] document retention and preservation practices"); Cunningham v. Std. Fire Ins. Co., No. 07-cv-02538-REBKLM, 2008 U.S. Dist. LEXIS 117304, 2008 WL 2668301, at *12–13 (D. Colo. Jul. 1, 2008) (holding that plaintiff's general assertion that he received fewer e-mails than expected in discovery was not sufficient to justify 30(b)(6) deposition on document preservation).

^{44.} See, e.g., Martin v. Allstate Ins. Co., 292 F.R.D. 361, 364 (N.D. Tex. 2013) ("While Plaintiff speculates that Defendant may have additional documentation that it has not produced, there is no evidence to support that supposition at this point."); Orillaneda v. French Culinary Inst., No. 07 Civ. 3206 (RJH)(HBP), 2011 WL 4375365, at *9 (S.D.N.Y. Sept. 19, 2011) (concluding that "discovery of defendant's search procedures and information systems . . . may be appropriate in certain circumstances, but it is not appropriate in this case unless and until plaintiff makes a specific showing that defendant's production is deficient"); In re Boxer Prop. Mgmt. Corp., No. 14-09-00579-CV, 2009 Tex. App. LEXIS 7279, at *18 (Tex. App.—Houston [14th Dist.] Sept. 3, 2009, orig. proceeding) ("Bare assertions that an opponent is hiding documents do not justify deposing in-house counsel at the courthouse about whether a diligent document search was really conducted."). But see Burnett v. Ford Motor Co., No. 3:13-cv-14207, 2015 U.S. Dist. LEXIS 88519, at *30–38 (S.D. W. Va. July 8, 2015) (explaining that "[c]ontrary to Ford's contentions, discovery of document retention and disposition policies is not contingent upon a claim of spoliation or proof of discovery abuses, and may be accomplished through a rule 30(b)(6) witness," and concluding that "Ford's generic objections to 'discovery on discovery' and 'non-merits' discovery are outmoded and unpersuasive").

duced or that was destroyed. Speculation that there is more will not suffice; if the theoretical possibility that more documents exist sufficed to justify additional discovery, discovery would never end."⁵⁰ Instead, a requesting party must at a minimum present evidence that "permit[s] a reasonable deduction that other documents may exist or did exist or have been destroyed."⁵¹ Of course, the hard part is often determining when allegations pass from mere speculation to evidence sufficient to permit a reasonable deduction of inadequate responses. The case law regarding this standard is "less than clear."⁵² Ultimately, courts must employ a case-specific analysis to evaluate requests for process-directed discovery based on all the circumstances of the case, including the course of conduct between the parties and the proportionality factors embodied in

rule 26.53

§ 16.3:3 Procedure for Resisting Process-Directed Corporate Depositions

Neither the federal rules nor the Texas rules set out a specific procedure for serving written objections to the topics identified in a corporate deposition notice. Thus, on receipt of a corporate deposition notice that seeks improper process-directed discovery, which fails to "describe with reasonable particularity the matters on which examination is requested," or is otherwise objectionable, a party's safest course is to seek relief from the court prior to the deposition by filing a motion for a protective order.⁵⁴

Federal Rule of Civil Procedure 26(c)(1) provides that a "court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden of expense."⁵⁵ A party seeking relief under the federal rules

52. See Schaffer, Deconstructing "Discovery about Discovery," at 216, 242–261 (describing different statements of evidentiary standards set out in relevant cases); (noting that the "challenge comes" in determining when process-directed discovery is "relevant and proportional to the needs of the case" and describing multiple relevant cases).

53. See Schaffer, Deconstructing "Discovery about Discovery," at 221 ("The court's role is to define and then ensure the appropriate scope of discovery based upon a case-specific inquiry.").

54. See Heartland Surgical Specialty Hosp., LLC v. Midwest Div., Inc., No. 05-2164-MLB-DWB, 2007 U.S. Dist. LEXIS 26552, at *11–12 (D. Kan. Apr. 9, 2007) (noting that a party had failed to file a motion for protective order regarding 30(b)(6) topics that included discovery-process issues).

^{50.} Hubbard, 247 F.R.D. at 29.

^{51.} Hubbard, 247 F.R.D. at 29; accord Orillaneda v. French Culinary Inst., No. 07 Civ. 3206 (RJH)(HBP), 2011 WL 4375365, at *6 (S.D.N.Y. Sept. 19, 2011) ("Indeed, the search and maintenance of a party's information systems may be relevant when a party can point to the existence of additional responsive material or when the documents already produced permit a reasonable deduction that other documents may exist or did exist and have been destroyed." (quotation marks omitted)); see also Rodriguez & Horan, Meta-Discovery, at 762–64 (arguing that process-directed discovery should require "some showing of a specific deficiency in the other party's production" and gathering relevant cases).

should keep in mind that the court is authorized to award the prevailing party its reasonable expenses incurred in either bringing or responding to a motion for protective order.⁵⁶ Similarly, under the Texas Rule of Civil Procedure 192.6(a), "[a] person from whom discovery is sought" may seek entry of a protective order "[t]o protect the movant from undue burden, unnecessary expense, harassment, annoyance, or invasion of personal, constitutional, or property rights," though a party "should not move for protection when . . . an assertion of privilege is appropriate."⁵⁷

§ 16.4 Corporate Deposition

§ 16.4:1 Notice of Deposition

Scope of Notice: As mentioned above, both the federal rule and the Texas rule require a corporate deposition notice to "describe with reasonable particularity" the matters on which testimony is requested.⁵⁸ "Reasonable particularity' requires the topics listed to be specific as to subject area and to have discernible boundaries."⁵⁹ "Where the topics concern 'discovery on discovery' and/or complex data, even greater specificity is required to ensure that a witness can prepare for the deposition, that the deposition is productive, and that the parties' time is not wasted on topics that do not relate to core claims or defenses."⁶⁰ Courts have suggested that the noticed party is not required to designate a witness unless the requesting party has met its burden of sufficiently identifying the deposition topics.⁶¹ After all, an overbroad corporate deposition notice subjects the responding party to the impossible task of identifying a witness to testify as to the outer limits of the noticed topics.⁶²

57. Tex. R. Civ. P. 192.6(a).

58. Fed. R. Civ. P. 30(b)(6); Tex. R. Civ. P. 199.2(b)(1).

59. Winfield v. City of New York, No. 15-2v-05236 (LTS) (KHP), 2018 U.S. Dist. LEXIS 22996, at *15 (S.D.N.Y. Feb. 12, 2018).

60. Winfield, 2018 U.S. Dist. LEXIS 22996, at *15.

61. Fed. R. Civ. P. 30(b)(6); *Dwelly v. Yamaha Motor Corp.*, 214 F.R.D. 537, 540 (D. Minn. 2003); *Prokosch v. Catalina Lighting, Inc.*, 193 F.R.D. 633, 638 (D. Minn. 2000); *Starlight Int'l Inc. v. Herlihy*, 186 F.R.D. 626, 639 (D. Kan. 1999).

62. Reed v. Bennett, 193 F.R.D. 689, 692 (D. Kan. 2000).

^{55.} Fed. R. Civ. P. 26(c)(1).

^{56.} Fed. R. Civ. P. 26(c)(3), 37(a)(5); see also 246 Sears Rd. Realty Corp. v. Exxon Mobil Corp., No. 09-CV-899 (NGG) (JMA), 2013 U.S. Dist. LEXIS 120506, at *3 (E.D.N.Y. July 26, 2013) (awarding attorneys' fees and costs for defendant where plaintiff alleged numerous deficiencies in defendant's document production and brought motion to compel discovery into defendants' search efforts without adequate basis).

In *Bowers v. Mortgage Electronic Registration Systems, Inc.*, the trial court reviewed a corporate deposition notice seeking testimony regarding "Quality Assurance and Data Integrity including the reporting systems including reconciliation between members."⁶³ The court found that this topic failed to identify with sufficient particularity what the noticing party was referring to and granted a motion for protective order.⁶⁴ Additionally, in *Mims-Johnson v. Bechtel National, Inc.*, the court reviewed a number of listed topics that began with "the prefatory language '[a]ll knowledge or information' or '[a]ll knowledge and information."⁶⁵ The trial court found that this language made the otherwise reasonable requests overly broad and struck such phrase from the categories, replacing it with "all information known or reasonably available to the organization."⁶⁶

Accordingly, when noticing a corporate deposition, a party must take care to specifically describe each of the e-discovery issues on which it is seeking testimony and avoid prefatory language that may make an otherwise specific request overly broad. A sample e-discovery corporate deposition notice is provided in the appendix at the end of this chapter.

Timing/Limitations: The advisory committee notes to Federal Rule of Civil Procedure 30 explain that "[a] deposition under rule 30(b)(6) should, for purposes of this [10-deposition] limit, be treated as a single deposition even though more than one person may be designated to testify."⁶⁷ Moreover, even if the officers and employees of a corporation have been deposed, a party may still seek to take a deposition of the corporation itself; doing so does not violate the rule prohibiting the deposition of a deponent who has already been deposed in the case.⁶⁸ "For the purpose of th[e] durational limit, the deposition of each person designated under rule 30(b)(6) should be considered a separate deposition," meaning that each deposition will be limited to one day of seven hours.⁶⁹

Under the Texas Rules of Civil Procedure, there is not a limit on the number of depositions a party may take. Instead, the total time for oral depositions is typically set at six hours per side under rule 190.2 (discovery level 1) and fifty hours per side under

- 65. No. CV-10-3119-RMP, 2012 WL 529896, at *3 (E.D. Wash. Feb. 16, 2012).
- 66. Mims-Johnson, 2012 WL 529896, at *3.
- 67. Fed. R. Civ. P. 30 advisory committee notes to the 1993 amendments.
- 68. See Fed. R. Civ. P. 30(a)(2)(A)(ii).
- 69. Fed. R. Civ. P. 30 advisory committee notes to the 2000 amendments; Fed. R. Civ. P. 30(d)(1).

^{63.} No. 10-4141-JTM, 2011 WL 6013092 at *6 (D. Kan. Dec. 2, 2011).

^{64.} Bowers, 2011 WL 6013092, at *6.

rule 190.3 (discovery level 2). Each deposition is typically limited to six hours per side, not including breaks.⁷⁰

§ 16.4:2 Selecting the Witness

If a process-directed corporate deposition is allowed, the testimony elicited can have a significant impact on the course of the lawsuit. For example, in *In re CV Therapeutics, Inc., Securities Litigation*, the defendant presented a "senior corporate counsel" to testify as a corporate witness on "the location of electronic data and back-ups" at the company.⁷¹ When he was asked whether "all the different drives" on the company's networks were being searched for responsive documents, he responded:

It's ongoing, so I believe, at this point—we started in November, and we're still slugging through it. There's a lot of data. I believe, at this point, the S drive and the H drive, perhaps the e-mail drive or the exchange server, have all been copied to allow for searching for potentially responsive communications to the document requests. We do intend to move through whatever servers we haven't yet gotten to, and it's possible there's a couple we haven't, because we're focused on areas where we would expect to find the most responsive documents.⁷²

Later in the lawsuit, the company sought a protective order to avoid having to search and review documents from these same drives, which the company estimated would take approximately ten months and cost over \$2.2 million.⁷³ The court denied the protective order and required a preliminary search of the drives, relying in part on the corporate witness's prior representation that the company intended to search these data sources.⁷⁴ This case demonstrates the extreme downside risk of suboptimal 30(b)(6) testimony and the corresponding importance of selecting and adequately preparing the right witness for a process-directed corporate deposition.

Select E-Discovery Witnesses Early: In cases that are likely to involve extensive e-discovery, parties should anticipate the possibility that requests for process-directed corporate depositions will be forthcoming and should consider at the outset of litigation who might be designated if such ciscovery is allowed. By identifying an individ-

- 71. No. 03-03709, 2006 U.S. Dist. LEXIS 28909, at *29 n.5 (N.D. Cal. Apr. 4, 2006).
- 72. In re CV Therapeutics, Inc., 2006 U.S Dist. LEXIS 28909, at *29 n.5.
- 73. In re CV Therapeutics, Inc., 2006 U.S Dist. LEXIS 28909, at *28-29 n.5.
- 74. In re CV Therapeutics, Inc., 2006 U.S Dist. LEXIS 28909, at *28-30.

^{70.} Tex. R. Civ. P. 199.5(c).

ual right away, the e-discovery witness can be involved in each step of the discovery process and, therefore, will be better prepared to provide testimony in the event of an e-discovery corporate deposition. In many cases, the selection of an appropriate corporate representative can avoid future motions for sanctions.

Technical Knowledge Preferable: An e-discovery witness will need to be knowledgeable about the format, location, and character of the organization's computer systems and ESI in order to provide appropriate testimony at the e-discovery corporate deposition. As explained above, the witness need not have personal knowledge regarding each topic identified in the rule 30(b)(6) notice but instead is permitted to provide testimony based on all matters "known or reasonably available to the organization."75 For that reason, it is generally preferred to choose a witness with a technical background rather than a layperson who may be more familiar with the litigation at issue. In the event a corporation outsources its IT needs, the rule 30(b)(6) witness may be a nonemployee vendor. Nontechnical witnesses often oversimplify e-discovery issues by making broad statements about what was or was not searched, the capabilities of the search mechanisms, and the extent to which ESI was preserved. As described above in the example of In re CV Therapeutics, Inc., Securities Litigation, such oversimplified testimony can have far-reaching and expensive consequences. By contrast, technical experts can make important distinctions about exactly what was done and why. It is easier to prepare a technical person to discuss the e-discovery issues than to train a nontechnical person about a company's computer systems and ESI. The technical person must, however, have a baseline knowledge of the claims and defenses at issue in order to provide context to various areas of inquiry.

Practice Tip: Clients often fail to recognize the importance of e-discovery corporate depositions and thus are reluctant to designate their valuable technical employees as witnesses. Don't fall into this trap. Though the initial costs may be higher, designating and preparing the appropriate witness for an e-discovery corporate deposition oftentimes will prevent costly discovery motions and, potentially, sanctions.

Parties May Designate More Than One Witness: Both Federal Rule of Civil Procedure 30(b)(6) and Texas Rule of Civil Procedure 199.2(b)(1) allow a party to designate more than one witness, if necessary, to provide sufficient testimony regarding each of the matters listed in the deposition notice.⁷⁶ When preparing for an e-discov-

^{75.} *PPM Fin., Inc. v. Norandal, USA, Inc.*, 392 F.3d 889, 894–95 (7th Cir. 2004); *Rodriguez v. Pat-aki*, 293 F. Supp. 2d 305, 311 (S.D.N.Y. 2003) ("[I]t is settled law that a party need not produce the organizational representative with the greatest knowledge about a subject; instead, it need only produce a person with knowledge whose testimony will be binding on the party.").

§ 16.4

ery corporate deposition, a party should consider each topic in the deposition notice before deciding how many witnesses to designate in response. Often, a single witness may not be available to testify about each topic listed. For example, a witness may be familiar with the party's computer systems but not with the particular software that contains relevant ESI. In some cases, the witness may be able to learn enough to testify regarding each topic, but in others that may be practically impossible.

Practice Tip: Meet with your corporate witnesses before they are actually designated to testify in response to a corporate deposition notice. In some cases, it will be impossible to determine whether a witness will be able to testify regarding the topics listed in the notice until you actually start preparing him for the deposition. If you wait until immediately before the deposition to begin preparing your witness, it may be too late to find an additional or substitute witness if additional witnesses are necessary to appropriately address each topic listed in the notice.

§ 16.4:3 Preparing the Rule 30(b)(6) Witness Duty of Responding Party

The entity receiving a rule 30(b)(6) deposition notice "must make a conscientious good-faith endeavor to designate the persons having knowledge of the matters sought by [the party noticing the deposition] and to prepare those persons in order that they can answer fully, completely, unevasively, the questions posed . . . as to relevant subject matters."⁷⁷ "[T]he duty to present and prepare a rule 30(b)(6) designee goes beyond matters personally known to that designee or to matters in which that designee was personally involved."⁷⁸ "The deponent must prepare the designee to the extent matters are reasonably available, whether from documents, past employees, or other sources."⁷⁹

If the designated witness (or a substitute witness) is still unable to testify about relevant facts, then "the appearance is, for all practical purposes, no appearance at all."⁸⁰ Therefore, the preparation of the witness or witnesses to respond as fully and completely as possible is vitally important in order to avoid incurring sanctions for producing an unprepared witness.

- 77. Brazos River Auth. v. GE Ionics, Inc., 469 F.3d 416, 433 (5th Cir. 2006).
- 78. Brazos River Authority, 469 F.3d at 433 (citation omitted).
- 79. Brazos River Authority, 469 F.3d at 433 (citation omitted).
- 80. Resolution Trust Corp. v. S. Union Co , Inc., 985 F.2d 196, 197 (5th Cir. 1993).

^{76.} Fed. R. Civ. P. 30(b)(6); Tex. R. Civ. P. 199.2(b)(1).

Testimony Based on Information "Known or Reasonably Available": Under both the federal rule and Texas rule, the corporate witness must be prepared to respond to a corporate deposition notice with information "known or reasonably available" to the entity.⁸¹ The rules, however, do not define the term "reasonably available."⁸² Some courts have compared the term to "possession, custody, or control" under Federal Rule of Civil Procedure 34.⁸³ By contrast, "reasonably accessible" under Federal Rule of Civil Procedure 26 defines the scope of the ESI to be produced absent court order. Regardless, the responding entity must gather all information responsive to the deposition notice that is in its custody, care, or control. "Even if the documents are voluminous and the review of the documents would be burdensome, the deponents are still required to review them in order to prepare themselves to be deposed."⁸⁴

This obligation may present questions unique to e-discovery where, for example, a party lacks details regarding how information is stored by its third-party vendors. On the other hand, courts have held that corporations are not required to obtain information from an affiliate for a rule 30(b)(6) deposition, particularly where the parent corporation has no direct involvement in the subject matter.⁸⁵ But if the corporation has control over the information requested in the notice it is obligated to provide that information, even if it is actually knowledge of an affiliate rather than that of the corporation.⁸⁶

Parties subject to a rule 30(b)(6) notice should carefully evaluate the availability of the specific information requested. This process should include not only attempts to gather all documentation within the entity's custody, care, and control, but also interviews of appropriate individuals to confirm that each of the matters listed in the notice is fully investigated and reviewed. To the extent a decision is made that certain infor-

85. See In re Ski Train Fire of Nov. 11, 2000 Kaprun Austria, No. MDL 1428(SAS)THK, 2006 WL 1328259, at *9 (S.D.N.Y. May 16, 2006) (finding that it is not reasonable to require a corporate parent to acquire all of the knowledge of its subsidiaries "on matters in which the parent was not involved" to testify to those matters during a rule 30(b)(6) deposition (emphasis added)).

86. See Twentieth Century Fox Film Corp. v. Marvel Enters., Inc., No. 01 CIV. 3016(AGS)(HB), 2002 WL 1835439, at *4 (S.D.N.Y. Aug. 8, 2002) ("[T]he responding party should be obligated to produce the information under its control," which is "consistent with the judicial interpretations of the other discovery provisions . . . [and] is also consistent with the purpose of discovery.").

^{81.} Fed. R. Civ. P. 30(b)(6); Tex. R. Civ. P. 199.2(b)(1).

^{82.} See Fed. R. Civ. P. 30(b)(6); Tex. R. Civ. P. 199.2(b)(1); see also Calzaturficio S.C.A.R.P.A. v. Fabiano Shoe Co., 201 F.R.D. 33, 38 (D. Mass. 2001) ("Neither rule 30(b)(6) itself nor the advisory notes nor reported case law addressing the rule define the terminology 'reasonably available."").

^{83.} See Calzaturficio S.C.A.R.P.A., 201 F.R.D. at 38.

^{84.} Concerned Citizens v. Belle Haven Club, 223 F.R.D. 39, 43 (D. Conn. 2004).

mation is not "reasonably available," the witness must understand the basis for such decision and be able to articulate it if challenged during the deposition.

Privilege Concerns in Witness Preparation: The risk of unintentionally waiving attorney-client privilege or work product is particularly problematic with designated corporate witnesses, who often have to be educated on noticed topics through information provided by others, including in-house and outside counsel. Courts have adopted varying approaches to deciding whether privilege is waived for documents reviewed by witnesses preparing for a corporate deposition, with some applying an "automatic waiver rule" and others applying a "case-by-case balancing test."⁸⁷ Counsel preparing a corporate witness must walk a fine line between adequately preparing the witness and protecting important privileged information.

§ 16.4:4 The Deposition Itself

During the deposition the corporate witness is expressly required to testify on behalf of the organization.⁸⁸ The Fifth Circuit has explained that in a corporate deposition an organization appears vicariously through its designated witness.⁸⁹ For that reason, a corporate witness should avoid testifying as to his personal knowledge or perceptions, as he is essentially testifying as to the organization's knowledge or perceptions.⁹⁰ And, as emphasized earlier, if the corporate representative is not prepared to testify about information "known or reasonably available to the organization," his appearance is, for all practical purposes, no appearance at all.⁹¹ If it becomes obvious that the corporate deposition representative is deficient, the corporation is obligated to provide a substitute.⁹²

Courts are split on whether a corporate witness must answer questions outside the scope of noticed topics but within the witness's personal knowledge.⁹³ A majority of courts, however, allow questioning outside the scope of the noticed topics, but hold

92. Marker v. Union Fidelity Life Ins. Co., 125 F.R.D. 121, 126 (M.D.N.C. 1989) (noting that even where defendant in good faith thought deponent would satisfy the deposition notice, it had a duty to substitute another person once deficiency of its designation became apparent during course of deposition).

^{87.} See Adidas Am., Inc. v. TRB Acquisitions LLC, 324 F.R.D. 389, 396–99 (D. Ore. 2017) (analyzing competing approaches to waiver question).

^{88.} Fed. R. Civ. P. 30(b)(6); Tex. R. Civ. P. 199.2(b)(1).

^{89.} Resolution Trust Corp. v. S. Union Co , Inc., 985 F.2d 196, 197 (5th Cir. 1993).

^{90.} Cutting Underwater Techs. USA, Inc. v. ENI U.S. Operating Co., 671 F.3d 512, 516 (5th Cir. 2012).

^{91.} Resolution Trust Corp., 985 F.2d at 197.

§ 16.4

that the witness's answers do not bind the organization.⁹⁴ Accordingly, the organization's attorney should object to questions outside the scope of the topics listed in the corporate deposition notice to make clear that the witness's responses are not binding on the organization.⁹⁵ Additionally, the organization's counsel must be prepared to object and instruct the witness not to respond to any questions delving into privileged matters.⁹⁶ Failure to do so will likely result in a waiver of the privilege, because a corporate witness waives the attorney-client privilege by testifying about portions of the attorney-client communication.⁹⁷ A corporate witness, however, should only be instructed not to answer a question in order to preserve a privilege, comply with a court order, or to secure a court order if the organization decides to suspend the deposition.⁹⁸

§ 16.5 Sanctions in the Context of Process-Directed Corporate Depositions

Failing to adequately prepare a witness for a corporate deposition can result in discovery sanctions.⁹⁹ Such sanctions arose in the context of process-directed discovery as early as 1989. In *Marker v. Union Fidelity Life Insurance Co.*, the plaintiff noticed a rule 30(b)(6) deposition covering details of the defendant's "general file keeping, storage, and retrieval systems."¹⁰⁰ The defendant's designated witness was "unable to answer specific questions concerning the retrieval of computerized data," and the

^{93.} *Cf. Detoy v. City & County of S.F.*, 196 F.R.D. 362, 365–67 (N.D. Cal. 2000) (analyzing issue and concluding that corporate witness may be questioned about any topic that is relevant under rule 26), with *Paparelli v. Prudential Ins. Co. of Am.*, 108 F.R.D. 727, 729–30 (D. Mass. 1985) (holding that the noticing party "must confine the examination to the matters stated 'with reasonably particularity' which are contained in the Notice of Deposition").

^{94.} See, e.g., Detoy, 196 F.R.D. at 365–67; McKinney/Pearl Rest. Partners, L.P. v. Metro. Life Ins. Co., 241 F. Supp. 3d 737, 752 (N.D. Tex. 2017) ("Such questions and answers are merely treated as the answers of the individual deponent.").

^{95.} See Detoy, 196 F.R.D. at 367 ("Counsel may note on the record that answers to questions beyond the scope of the rule 30(b)(6) designation are not intended as the answers of the designating party and do not bind the designating party.").

^{96.} Fed. R. Civ. P. 30(c)(2); Tex. R. Civ. P. 199.5(f).

^{97.} See Nguyen v. Excel Corp., 197 F.3d 200, 206-07 (5th Cir. 1999).

^{98.} Fed. R. Civ. P. 30(c)(2); Tex. R. Civ. P. 199.5(f); *Mass Engineered Design, Inc. v. Ergotron, Inc.*, No. 206 CV 272, 2008 WL 8667511, at *1 (E.D. Tex. Jan, 8, 2008) ("It is improper to instruct a deponent not to answer questions because the questions are outside the scope of a 30(b)(6) designation.").

^{99.} See Citgo Petroleum Corp. v. Seachem, No. H-07-2950, 2013 WL 2289951 (S.D. Tex. May 23, 2013) (granting monetary sanctions against a party for failing to adequately prepare its witness for a rule 30(b)(6) deposition). Discovery sanctions are addressed in more detail in chapter 15 of this book.

^{100. 125} F.R.D. 121, 125 (M.D.N.C. 1989).

defendant refused to produce another witness to address the topic.¹⁰¹ The court concluded that the defendant had failed to meet its obligations under rule 30(b)(6), warranting sanctions under rule 37.¹⁰² The court ultimately required the defendant "to produce such knowledgeable persons so that plaintiff may complete the deposition," and to either pay for plaintiff's counsel's travel to the deposition or present the witness in the venue of the lawsuit.¹⁰³

Courts have imposed similar sanctions in more recent cases involving processdirected corporate depositions. In Illiana Surgery & Medical Center, LLC v. Hartford Fire Insurance Co., the U.S. District Court for the Northern District of Indiana considered sanctions requested by the plaintiff after a "tumultuous course of discovery" that spanned nearly six years.¹⁰⁴ Following an earlier award of sanctions for the defendant's failure to produce claim file documents, the plaintiff noticed a rule 30(b)(6) deposition to address "the method by which [the defendant] maintained its electronic information over the course of [the plaintiff's] claim" and the defendant's efforts "to locate and produce all electronic documents."105 The defendant opposed the deposition, forcing the plaintiff to file a motion to compel, which the court granted.¹⁰⁶ The defendant designated an in-house attorney for the deposition. Although the witness was "familiar with [the company's] ESI process because of his role as litigation manager," he "did not participate in [the defendant's] efforts to produce documents to [the plaintiff] in this case," nor did he "talk to document custodians about what documents they had or how the documents had been gathered, ... review [the plaintiff's] discovery requests, . . . [or] review any documents produced in response to [the plaintiff's] discovery requests."107 The court concluded that, although the witness had engaged in some preparation, "it d[id] not appear that he was prepared to address the issues set forth in the notice of deposition."108 The court denied the death penalty sanctions sought by the plaintiff, but it ordered the defendant to produce a new witness and to "pay all costs associated with [the plaintiff's] motion as well as any additional costs and fees associated with discovery related to [the defendant's] late production of documents and failure to present a prepared deponent."¹⁰⁹

^{101.} Marker, 125 F.R.D. at 125-26.

^{102.} Marker, 125 F.R.D at 126.

^{103.} Marker, 125 F.R.D. at 126-27.

^{104.} No. 2:07-CV-003-JVB-APR, 2013 U.S. Dist. LEXIS 70153, at *2, *13 (N.D. Ind. May 16, 2013).

^{105.} Illiana Surgery & Medical Center, LLC, 2013 U.S. Dist. LEXIS 70153, at *5, *16.

^{106.} Illiana Surgery & Medical Center, LLC, 2013 U.S. Dist. LEXIS 70153, at *5, *16.

^{107.} Illiana Surgery & Medical Center, LLC, 2013 U.S. Dist. LEXIS 70153, at *6-7.

^{108.} Illiana Surgery & Medical Center, LLC, 2013 U.S. Dist. LEXIS 70153, at *15.

In Hoffman v. L&M Arts, the U.S. District Court for the Northern District of Texas imposed sanctions related to one of two e-discovery corporate witnesses.¹¹⁰ As with many sanctions cases, *Hoffman* involved a series of discovery disputes, during which the plaintiff obtained two separate orders for the defendant to designate witnesses for process-directed corporate depositions.¹¹¹ The first deposition was ordered after the court found that the defendant had "an extensive history of misconduct in [discovery]."¹¹² But at the deposition it "became apparent that [the witness] was not competent to testify about [the defendant's] information technology systems or its document collection and production process."113 The plaintiff therefore moved to compel a second corporate deposition, which the court granted, and requested sanctions, which the court deferred until after trial.¹¹⁴ The plaintiff again moved for sanctions after the second corporate deposition, arguing that the new witness also was not competent to testify regarding a number of discovery-process issues.¹¹⁵ The court took up both motions for sanctions after the plaintiff prevailed at trial.¹¹⁶ The court found that the first corporate witness was unable to answer questions within the scope of the 30(b)(6) topics that had been ordered by the court, entitling the plaintiff to recover attorneys' fees and costs related to the deposition.¹¹⁷ The court denied sanctions as to the second corporate deposition, though, because the second witness had provided complete answers on many of the noticed topics; "[h]e testified at length about [the defendant's] IT systems, including its backup and retention systems, and about the searches he performed for [the defendant] in connection with this case."¹¹⁸ Although the second witness had not been able to answer every question posed, the court concluded that the deposition transcript showed the witness "was adequately prepared to answer questions on the noticed deposition topics."119 Hoffman therefore demonstrates that perfection is not required, and sanctions likely are not warranted unless a witness is so ill-prepared that the deposition is "tantamount to a failure to appear."¹²⁰

- 109. Illiana Surgery & Medical Center, LLC, 2013 U.S. Dist. LEXIS 70153, at *17-18.
- 110. No. 3:10-CV-0953-D, 2015 U.S. Dist. LEXIS 27783 (N.D. Tex. Mar. 6, 2016).
- 111. Hoffman, 2015 U.S. Dist. LEXIS 27783, at *3-8.
- 112. Hoffman, 2015 U.S. Dist. LEXIS 27783, at *3-4.
- 113. Hoffman, 2015 U.S. Dist. LEXIS 27783, at *3-4.
- 114. Hoffman, 2015 U.S. Dist. LEXIS 27783, at *4-5.
- 115. Hoffman, 2015 U.S. Dist. LEXIS 27783, at *6-7.
- 116. Hoffman, 2015 U.S. Dist. LEXIS 27783, at *9.
- 117. Hoffman, 2015 U.S. Dist. LEXIS 27783, at *13-14.
- 118. Hoffman, 2015 U.S. Dist. LEXIS 27783, at *14.
- 119. Hoffman, 2015 U.S. Dist. LEXIS 27783, at *15-16.

Appendix

Appendix Sample Corporate Deposition Notice

IN THE UNITED STATES DISTRICT COURT FOR THE _____ OF TEXAS

	§
	§
Plaintiff,	§
	§
VS.	§ CIVIL ACTION NO
	§
,	§
Defendant.	§
	ş

NOTICE OF INTENTION TO TAKE DEPOSITION OF [NAME OF ORGANIZATION]

PURSUANT TO FEDERAL RULE OF CIVIL PROCEDURE 30(b)(6)

Please take notice that, pursuant to rule 30(b)(6) of the Federal Rules of Civil Procedure, [plaintiff/defendant] will take the deposition on oral examination under oath of [name of organization] at [date, time, location]. The deposition will be recorded both stenographically by a certified court reporter and by a licensed videographer and will continue from day to day until concluded, with such adjournment as to time and place as may be necessary.

^{120.} *Hoffman*, 2015 U.S. Dist. LEXIS 27783, at *16 ("Although [the plaintiff] may have been entitled to answers on these questions, she is not entitled to sanctions.").

Appendix

Pursuant to rule 30(b)(6) of the Federal Rules of Civil Procedure, [name of organization] must designate one or more persons to testify about information known or reasonably available to [name of organization] regarding the following topics:

- 1. The existence, nature, custody, condition, and location of electronically stored information (ESI), documents, and tangible things regarding [subject matter of litigation].
- 2. The type, number, and location of all servers, workstations, laptops, and other devices used at any point in time to access, store, or utilize ESI regarding [subject matter of litigation].
- 3. The type of user workstation systems and client programs in use during the relevant time period.
- 4. Polices or procedures related to employee or agent use of hand-held computing devices for business purposes.
- 5. The operating system(s), file storage program(s), and other software application(s) used with respect to any ESI regarding [subject matter of litigation].
- 6. The type, format, and location of all backup systems that may contain ESI regarding [subject matter of litigation].
- 7. The organization's policies in effect during the relevant time period with respect to the organization, storage, archiving, backup, or deletion of ESI.
- 8. The identity of the organization's current and former employees responsible for the management, organization, storage, or deletion of ESI during the relevant time period.
- 9. The identity of the organization's current and former employees that have or have had access to the computers used at any point in time to access, store, or utilize ESI regarding [subject matter of litigation].
- 10. The organization's policies with respect to e-mail creation, maintenance, and storage during the relevant time period.
- 11. The types of computers, work stations, and handheld or portable electronic devices used during the relevant time period by each person identified in your rule 26(f) disclosures as having knowledge of relevant facts regarding [subject matter of litigation].
- 12. The locations outside the organization where electronic documents are regularly sent.

- 13. Modifications to the use of your computers or servers since receipt of the notice of litigation (legal hold notice).
- 14. Legacy data regarding [**subject matter of litigation**] acquired by the organization through the acquisition of another company or companies.
- 15. The use of an intranet, extranet, website, or cloud storage that contains the organization's records, document, databases, or other information.
- 16. The organization's voice mail systems and the organization's policies with respect to the use and retention of voice mail data.
- 17. The organization's document retention plan in use during the relevant time period for both hard-copy materials and ESI.
- 18. The organization's efforts to preserve ESI regarding [subject matter of litigation].
- 19. The organization's efforts to collect ESI regarding [subject matter of litigation].
- 20. The organization's efforts to review ESI regarding [subject matter of litigation].
- 21. The organization's efforts to produce ESI requested by [name of noticing party].

DATED:

[Name of attorney] State Bar No.: [E-mail address] [Address] [Telephone] [Fax]



Chapter 17

Mediation of E-Discovery Disputes and Special Masters

Peter S. Vogel and Allison O. Skinner

§ 17.1 Introduction

As most readers can attest, discovery is generally a contentious experience. It is the duty of each lawyer to zealously pursue evidence to help prove his client's case or disprove the case of the opponent—sometimes both, depending upon the case. Also, rarely do lawyers communicate well with the client's information technology ("IT") leaders, such as the chief information officer ("CIO"), chief technology officer ("CTO"), Chief Information Security Officer ("CISO"), or Chief Privacy Officer ("CPO"). This isn't because of a lack of interest or concern, but is because CIOs, CTOs, CISOs, and CPOs see the world much differently than lawyers do, not to mention that they speak a different language, that of technology, not law.

CIOs, CTOs, CISOs, and CPOs are primarily interested in protecting the IT environment and data from disasters and cyber intrusions. These disasters may be caused by the natural failure of IT, because every component with a computer is built with a mean time between failure. That is, each component part of every computer has an expected life and will then fail. Or they may be caused by internal users' mistakes, external criminal cyberattacks, or phenomena such as Internet failure because of sunspots. Sometimes accidents happen. For example, a flood on the thirty-third floor of Wells Fargo Plaza in Houston flooded Gardere's computer room. Gardere's CIO had weathered Hurricane Katrina in 2005, so he was prepared for such an event. As a result, Gardere did not experience any loss in data.

It goes without saying that lawyers and judges are not trained as IT professionals, and because of the resulting language barriers, lawyers and the client's IT professionals often miscommunicate. This leads to lawyers misunderstanding the electronic evidence ("e-evidence") that may be available or unavailable in any particular case. As a result, the discovery process does not always work as simply as back when all evidence was in paper.

The bottom line is that there are opportunities for lawyers, IT professionals, and judges to misunderstand and miscommunicate about e-evidence. Accordingly, the use of third-party neutrals ("e-neutrals") may be an effective way for litigants to better manage e-evidence and therefore electronic discovery ("e-discovery"). The two primary uses of the e-neutrals are e-mediation and appointment of special masters.

The e-mediation process allows for confidential caucuses between the party, lawyers, IT leader, and e-mediator. The appointment of an e-neutral special master permits a judge to send complicated technical e-evidence and e-discovery matters to an individual who understands the IT issues and legal issues and who can act on behalf of the court to resolve disputes.

§ 17.2 The E-Mediator

When the concept of mediation was introduced in Texas with the passage of the 1987 Alternative Dispute Resolution Act, it was adopted into the mainstream practice of law for the purpose of settling an entire case. In reality, the purpose of mediation is to facilitate the resolution of any dispute, whether before or during litigation.

Every lawsuit now has some form of electronic evidence—e-mails, texts, GPS (global positioning system) data, spreadsheets, social media postings, and word-processing documents, to name a few. Discovery battles are at the heart of every lawsuit, so it makes sense that mediation is appropriate for resolving discovery disputes.

§ 17.3 E-Mediation

When e-discovery is involved, the mediation is referred to as an e-mediation, and the e-neutral is called an e-mediator. An e-mediator is trained and experienced in not only dispute resolution, but ESI. An e-mediation provides the following benefits:

- Self-directed workable solutions
- Defining scope parameters
- Determining relevancy
- Determining reasonable accessibility of ESI
- Creating timelines for production and e-dispositions
- Proposing confidential compromises
- Creating efficiencies with a mutual discovery plan

- Setting guidelines for asserting violations of the discovery plan
- Creating boundaries for preservation
- Avoiding spoliation pitfalls
- Defining proportionality
- Determining forms of production
- Identifying custodians/key players
- Managing protection of privileged information
- Maintaining credibility with the court
- Encouraging client participation and buy-in
- Avoiding court-imposed sanctions
- Cost allocation¹

Parties should use e-mediation at the outset of a case to develop the mediated e-discovery plan. If the parties did not develop a discovery plan, however, they can use emediation at a later date for a specific dispute, such as a search protocol. Using an emediator on an issue-by-issue basis² allows for informal negotiations on an as-needed basis. Efficiency is created when the parties have access to an e-mediator who is familiar with the pretrial activities to address specific issues in a timely manner.³ Additionally, e-mediation allows the parties to maintain civility and avoid a breakdown in communication. Maintaining a working relationship among counsel and their respective clients may be an important consideration, particularly if a business relationship is involved.

The e-mediation may begin with the parties in the same room with the e-mediator.⁴ The e-mediator may split the parties into respective caucus rooms as necessary.⁵ A

- 4. Skinner, How to Prepare a Mediation Statement.
- 5. Skinner, How to Prepare a Mediation Statement.

^{1.} Allison O. Skinner, The Role of Mediation for ESI Disputes, 70 Ala. Law. No. 6, 425 (2009).

^{2.} Allison O. Skinner, *How to Prepare a Mediation Statement for An E-Discovery Mediation*, DRI E-Discovery Connection Newsletter (DRI, Chicago, III.), 2010, http://clients.criticalimpact.com/ newsletter/newslettercontentshow1.cfm?contentid=1453&id=250.

^{3.} An added benefit of using an e-mediator is that the neutral is educated on the facts of the case and may be appropriate to use as the settlement mediator for case disposition. This familiarity with the parties and the issues should enhance the neutral's ability to settle the case. However, the parties may not want to use the e-mediator for settlement purposes for strategic reasons, such as not wanting the settlement mediator to know confidential information that was divulged to the e-mediator.

major advantage to using e-mediation is that the client representative and an IT representative participate in the negotiations of developing the mediated e-discovery plan ("MEP") in a confidential environment. This opportunity provides a forum to educate the stakeholders on the ESI issues.⁶ Consequently, e-mediators are trained and experienced in both mediation and e-discovery.⁷ Because the e-mediator is facilitating mutual solutions among the parties, by virtue of the process, the parties are demonstrating good faith as required under the parties' Federal Rule of Civil Procedure 26 obligations.

§ 17.4 The E-Mediation Statement

In an e-mediation, the parties prepare an e-mediation statement,⁸ and the outcome of the mediation is memorialized in an MEP.⁹

Parties and their counsel should view an e-mediation differently from a typical mediation used to settle a case.¹⁰ After all, the parties cannot reach trial without completing discovery. To prepare for an e-mediation, counsel should be prepared to address the following issues candidly and confidentially in the e-mediation statement.

§ 17.4:1 Participants

Counsel should identify who is available to participate in the e-mediation. Preferably, the in-house counsel or client representative with authority to make final decisions on behalf of the client should attend with outside counsel and an IT representative. Counsel should advise the mediator whether the IT representative is a company employee or a hired consultant. If the IT representative is a hired consultant, a brief background about the IT representative's experience with the client's business is helpful. Further, counsel should identify whether any corporate representative depositions have been taken addressing custodial issues of ESI e-depositions. If portions of a deposition transcript would be helpful to the mediator to understand the types of ESI the client maintains, counsel should provide those relevant portions of the deposition transcript.

- 8. Skinner, How to Prepare a Mediation Statement.
- 9. Skinner, How to Prepare a Mediation Statement.
- 10. Skinner, How to Prepare a Mediation Statement.

^{6.} Skinner, How to Prepare a Mediation Statement.

^{7.} American College of e-Neutrals, What is the American College of e-Neutrals?, www.acesin.com.

§ 17.4:2 What to Provide

Counsel should provide all relevant or applicable discovery requests, objections, responses, motions to compel (with exhibits), motions for protective order (with exhibits), applicable discovery orders, and Federal Rule of Civil Procedure 16 scheduling orders. In certain circumstances, the applicable litigation hold letter or preservation letter should be provided. Counsel should identify whether every request is in dispute or only certain groups of requests. Grouping requests by similar issues (which may not be in chronological order) facilitates the issue-based aspect of an e-mediation.

§17.4:3 Approach

If requests can be grouped by issue, counsel should identify the issue and the position their client takes with respect to that issue. If the e-mediation will address every request in a set of discovery, counsel should identify themes or issues in which they anticipate the parties will share differences. Counsel should articulate the grounds that support their position for a particular theme or issue and whether any points of concession are available. This part of the position statement should also include issues or themes counsel anticipates the opposing side will have. For a requesting party, counsel should be able to provide why a particular issue is relevant.

§17.4:4 Mapping

Counsel should be prepared to discuss in confidence with the mediator a general overview of the client's data mapping. Data mapping traces the connection from the communicator and the methodology of the communication. This connection may run unidirectionally or bidirectionally. A data map should include storage devices, methodologies, technologies, systems, applications, custodians, communicators, and retention policies. A data map is like an organizational chart for the digital age. Counsel should be aware of and identify any virtualization or clouding. In other words, a data map traces the identities of any entities that are not named parties but by virtue of their relationships to the client maintain or have connections to discoverable electronic information.

§ 17.4:5 Spoliation

Counsel should identify whether any spoliation pitfalls exist.

§ 17.4:6 Costs

Counsel should identify any known cost or burden concerns.

§ 17.4:7 Timing

Counsel should articulate any relevant timing issues. Production of e-discovery can be time-consuming, and it is important to be aware of any timing issues that may run afoul of any agreement or order on production.

§ 17.4:8 Privilege

Counsel should identify any privilege concerns. Additionally, counsel should provide their position on how inadvertent disclosure of privileged information should be handled. Restated, counsel should articulate how their client would like to handle any issues falling under Federal Rule of Evidence 502.

§ 17.4:9 Compatibility

Counsel should discuss any issues relating to the compatibility of the client's electronic information or the capability of producing it and providing it to the law firm, the opposing party, or the opposing law firm.

§ 17.4:10 Inaccessibility

If counsel is aware of any requested ESI that counsel believes is relevant and in existence but that is reasonably inaccessible, counsel should identify the information and explain why the information is inaccessible.

§ 17.4:11 Searches

Searches must be conducted to identify and retrieve discoverable information. Most commonly, searches for e-mails, texts, or voice mails are requested, for example. For different types of data, counsel should identify keywords or search terms their client believes are reasonably calculated to identify relevant information. Conversely, counsel should provide a list of keywords, if aware of any, that counsel believes are inappropriate and explain why. Further, if other search concepts are appropriate, like "fuzzy logic," then counsel needs to be prepared to discuss this alternative.

§ 17.4:12 E-Discovery Experience

Counsel should confidentially communicate (in a manner they are comfortable with) their level of knowledge or expertise in handling e-discovery as well as their level of knowledge regarding their client's particular technologies. The e-mediator recognizes that the bar in general, along with parties, has a learning curve. The e-mediator also recognizes that the mediation forum is an opportunity for counsel, in-house counsel, and the IT representative to focus on the specific case and the related discovery issues together.¹¹

The e-mediation statement is similar to providing the procedure, facts, and law to the mediator in a settlement mediation.¹²

§ 17.5 Selecting an Appropriate E-Mediator

E-mediation is a tool to manage the complexity of electronic evidence while preserving judicial economy. A successful e-mediation, however, requires the right e-mediator. An e-mediator should be trained and experienced not only in e-discovery but in alternative dispute resolution. It is important to note that the Supreme Court of Texas adopted ethical guidelines for mediators in 2005.¹³ An e-mediator should be versed in these guidelines or similar ethical standards if the e-mediator is from out of state. Beware of the e-discovery vendor who has not had the requisite training and experience as a mediator because they may unwittingly violate the mediative process. In certain types of cases, the parties may want the e-mediator to also have specialized industry knowledge in a particular practice area, for example, aviation, gaming, or pharmaceuticals. The American College of E-Neutrals, **www.acesin.com**, offers a two-day program designed to teach neutrals how to mediate e-discovery disputes. Other e-mediation training programs are available, and attorneys should require the emediator have some type of training in these fields.

§ 17.6 The Effect of E-Mediation on the Cost of E-Discovery

E-mediation should reduce, not add to, the cost of e-discovery. E-mediator charges at customary rates pale in comparison to endless e-discovery battles and motion prac-

^{11.} Skinner, How to Prepare a Mediation Statement.

^{12.} Skinner, How to Prepare a Mediation Statement.

^{13.} See Texas Mediator Credentialing Association, Standards of Practice and Code of Ethics, https://www.txmca.org/index.php?page=10.

tice. E-mediation conserves time and cost because the parties have a plan. Also, having access to an e-mediator allows parties to reach a resolution sooner than they would be able to setting a hearing on an overburdened court docket.

E-mediation is a unique, confidential venue available to lawyers, clients, and the court to efficiently manage the discovery of electronic evidence. E-mediation allows parties to demonstrate cooperation and communicate in a safe environment to reach resolution so a case may be resolved on its merits.

E-mediation is a tool that Texas lawyers should consider as a method for managing ediscovery, which will reduce the time, money, and energy of e-discovery motion practice.

§ 17.7 E-Neutral Special Masters

§ 17.7:1 In General

The appointment of a special master under Texas Rule of Civil Procedure 171 or Federal Rule of Civil Procedure 53 is another viable method of alternative dispute resolution to resolve e-discovery disputes.¹⁴ Under Texas Rule of Civil Procedure 171 and Federal Rule of Civil Procedure 53, the order appointing the special master is required to include provisions that address the scope of the appointment, the special master's duties and authority, provisions for ex parte communications, filing materials, standard of review, setting compensation, and issuing orders.

In 2016, the Lawyers Conference of the American Bar Association (ABA) Judicial Division formed a Committee on Special Masters to promote research and education concerning special masters and to make proposals concerning using their use. This committee concluded that one of the difficulties faced by both courts and practitioners is the lack of a methodical and consistent approach to the appointment and use of special masters.

In January, 2019, the ABA House of Delegates approved the Committee on Special Masters' ABA Guidelines for the Appointment and Use of Special Masters in Federal and State Civil Litigation¹⁵ as follows:

^{14.} See Honorable Shira A. Scheindlin and Jonathan M. Redgrave, Special Masters and E-Discovery: The Intersection of Two Recent Revisions to the Federal Rules of Civil Procedure, 30 Cardozo L. Rev. 347 (2008).

Consistent with the Federal Rules of Civil Procedure or applicable state court rules:

- (1) It should be an accepted part of judicial administration in complex litigation (and in other cases that create particular needs that a special master might satisfy) for courts and the parties to consider using a special master and to consider using special masters not only after particular issues have developed, but at the outset of litigation.
- (2) In considering the possible use of a special master, courts, counsel, and parties should be cognizant of the range of functions that a special master might be called on to perform and roles that a special master might serve.
- (3) In determining whether a case merits appointment of a special master, courts should weigh the expected benefit of using the special master, including reduction of the litigants' costs against the anticipated cost of the special master's services, in order to make the special master's work efficient and cost effective.
- (4) Participants in judicial proceedings should be made aware that special masters can perform a bread array of functions that do not usurp judicial functions, but assist them. Among the functions special masters have performed are:
 - a. discovery oversight and management, and coordination of cases in multiple jurisdictions;
 - b. facilitating resolution of disputes between or among coparties;
 - c. pretrial case management;
 - d. advice and assistance recuiring technical expertise;
 - e. conducting or reviewing auditing or accounting;
 - f. conducting privilege reviews and protecting the court from exposure to privileged material and settlement issues; monitor-ing; class administration;
 - g. conducting trials or mini-trials upon the consent of the parties;
 - h. settlement administration;

^{15.} See www.americanbar.org/content/dam/aba/directories/policy/midyear-2019/100 -midyear-2019.pdf.

- i. claims administration; and
- j. receivership and real property inspection.

In these capacities special masters can serve numerous roles, including management, adjudicative, facilitative, advisory, information gathering, or as a liaison.

- (5) Courts should develop local rules and practices for selecting, training, and evaluating special masters, including rules designed to facilitate the selection of special masters from a diverse pool of potential candidates.
- (6) Courts should choose special masters with due regard for the court's needs and the parties' preferences and in a manner that promotes confidence in the selection process by helping to ensure that qualified and appropriately skilled and experienced candidates are identified and chosen.
- (7) The referral order appointing the special master should describe the scope of the engagement, including, but not limited to, the special master's duties and powers, the roles the special master may serve, the rates and manner in which the special master will be compensated, power to conduct hearings or to facilitate settlement, requirements for issuing decisions and reporting to the court, and the extent of permissible ex parte contact with the court and the parties. Any changes to the scope of the referral should be made by a modification to the referral order.
- (8) Courts and the bar should develop educational programs to increase awareness of the role of special masters and to promote the acquisition and dissemination of information concerning the effectiveness of special masters.
- (9) Courts and, where applicable, legislatures should make whatever modifications to laws, rules, or practices that are necessary to effectuate these ends.

The Scheindlin-Redgrave article succinctly describes four roles the special master may serve for ESI disputes: (1) facilitative, (2) compliance, (3) adjudicative, and (4) technical assistance.¹⁶ The facilitative role is similar to the role of an e-mediator, but the special master still has court authority, and the discussions are not confidential.

^{16.} Scheindlin & Redgrave, Special Masters and E-Discovery, at 383-87.

The role of a special master who oversees compliance of a court order allows for efficient case management by monitoring the parties' progress. In the role of adjudicator, the special master decides e-discovery issues. A special master who provides technical expertise, which may be particularly important in copyright or patent infringement cases, for example, requires a sophisticated level of technical knowledge relative to the subject matter. Regardless of the function of the special master, the needs of the case are addressed in an efficient manner, and the special master frees the court's time for dispositive matters.

One important option for special masters is that they may have ex parte conferences with different parties if permitted by the terms of the order. It might seem counterintuitive at first that a special master can have ex parte meetings with litigation parties while a judge may not. The following is an example of why ex parte meetings make sense.

§ 17.7:2 Example of Special Master in E-Discovery

In a particular case in a Texas state court, the judge appointed a special master regarding e-evidence concerning a 1985 computerized invoicing system and the 2000 SAP database (see the order included as an appendix to this chapter). The plaintiff alleged that the 1985 invoicing system contained detail records of the item numbers for each invoice of computer printers (the newly created 2000 SAP database did not contain the detail for each item sold, only the total dollar amount of each invoice).

The special master had ex parte meetings with the defendant to review the 1985 computer invoicing system and the 2000 SAP database. During the ex parte meeting with the defendant the special master requested copies of the data files so an independent examination by the special master could be conducted and the defendant would not see the examination. During the special master's examination of the 1985 invoicing records and the 2000 SAP database, the special master concluded that the 1985 computer system did not contain item details, only summary totals. As a result, data files were converted from the old 1985 system to the 2000 SAP system and contained the identical records.

By permitting the special master ex parte access to the defendant's computer, there was no disclosure of unrelated confidential evidence to the plaintiff. Also, the special master was able to access computer records to permit an independent review.

§ 17.8

§ 17.8 Conclusion

Lawyers, clients, and courts are looking for innovative ways to conserve time, money, and heartache for discovery disputes involving electronically stored information. Using alternative dispute resolution like e-mediation and special master appointments is an innovative approach that in the right cases has proved successful.

§ 17.9 Additional Resource

• Garrie, Daniel B, and Yoav M. Griver. *Dispute Resolution and E-Discovery*. Eagan, MN: Thomson Reuters, 2013.

Mediation of E-Discovery Disputes and Special Masters

Appendix

Appendix

CAUSE NO. CC-03-11791D

MICRO ELECTRONICS, INC. d/b/a MICRO CENTER,	\$ \$	COUNTY COURTATLAW
Plaintiff;	\$	
v.	9 9 9	NO.4
UMAX TECHNOLOGIES, INC. d/b/a UMAX TECHNOLOGIES, <i>Defendant.</i>	\$ \$ \$	DALLAS COUNTY, TEXAS

ORDER OF REFERENCE AND APPOINTMENT OF SPECIAL MASTER

BASED ON THE PLEADINGS and other case papers in this case and as a result of the hearing on November 12, 2004 on Plaintiff's ("Micro Center") Second Set of Discovery Motions Against Defendant ("UMAX") as well as the argument presented to this Court on a number of issues in dispute, the Court, pursuant to the provisions of *Texas Rules of Civil Procedure ("TRCP") Rule 171*, hereby orders that Peter Vogel is appointed as a Special Master (the "Special Master") for certain discovery issues in this case asserted in the Plaintiff's First and Second Set of Discovery Motions (the "Discovery Motions") to be paid a reasonable fee charged as taxable costs, to be initially assessed equally to the parties herein, subject to further orders of the court.

The Court determines that these discovery and computer issues require special expertise and that these issues create exceptional circumstances and good cause for the appointment of Master. Those discovery issues presented to the Special Master shall include review and analysis of, and reporting the Special Master's conclusions to the Court and counsel for all parties, about the following matters:

1. All of the matters relating to databases, invoicing, and transactional records contained in Micro Center's Second Set of Discovery Motions and those matters held in abeyance at the time of the Court's hearing on Plaintiff. Micro Center's First Set of Discovery Motions, including but not limited to the review and analysis of:

- Various computer and hardware and software systems ("Computer Systems") of UMAX Technologies, Inc. ("UMAX");
- B. Data stored on the various Computer Systems of UMAX, whether in databases or any other types of media or files,
- C. Creating, or having created, mirror images of certain computer storage media including, data and files, and related reviews of the contents of the mirror images of the Computer Systems of UMAX;
- D. The nature, configuration, capabilities and compatibility of UMAX's Platinum, SAP, and any other computer hardware and software systems ("Computer Systems');
- E. The nature, extent, size, and amount of data stored on those various Computer Systems, whether in databases or any other type of files maintained by UMAX;
- F. The ability, feasibility, and estimated costs of creating, or having created, mirror images of computer storage media containing database, data and files of UMAX in ea.ch of its Platinum and SAP databases and files related to transactions between Micro Center and UMAX, and related reviews of the contents of the mirror images of those UMAX files and records from UMAX's databases, and images of the software necessary to access, read, utilize and print the data;
- G. The feasibility and estimated costs associated with accessing UMAX's Platinum database and preparing and printing records and reports, including, but not limited to invoices, credit memos, e-mails, contracts, correspondence, check record histories, ledgers and subledgers (including accounts receivable and notations related thereto) and other transactions and records regarding Micro Center (all of which are referred to collectively as "Transactional Records") of transactions between UMAX and Micro Center from OMAX's Platinum database and lists of UMAX ledger and subledger accounts, and descriptions of their contents;
- H. The ability of UMAX to review, access, and print data and records, including, but not limited to invoices, credit memos, e-mails, contracts, correspondence, check record histories, ledgers and subledgers (including accounts receivable and notations related thereto) and other transactions and records regarding Micro Center, (all of which are referred to collectively as "Transactional Records") and other data (including metadata and revisions of Transactional Records) maintained by UMAX in both its Platinum and SAP databases and computers;
- I. The estimated costs of accessing and printing in original format, or if not available in original format, in other available alternative formats, Transactional Records and other data (including metadata and revisions of Transactional Records) from UMAX's Platinum and SAP databases and computers;
- J. Whether UMAX can currently print in original or other formats copies of invoices, credit memos, Transactional Records and other documents and records from its Platinum database which depict and/or describe commercial transactions and the documentation of those transactions between UMAX and Micro Center during the period of January, 1996 through December, 2001; and if it is

determined that UMAX carnot print those records, what the estimated costs are for a third party contractor to do so;

- K. Whether UMAX has the capability and can currently provide access to Micro Center and its counsel to Transactional Records and other data (including metadata and revisions to Transactional Records) from its databases (both Platinum and SAP) limited only to commercial transactions and the documentation of those transactions between UMAX and Micro Center during the period of 1996-2004; and if it cannot, what the estimated costs would be to furnish Micro Center with access to such data and records and the ability to read and print such data and records; and,
- L. What the estimated costs are for UMAX to furnish Micro Center and its counsel with legible and printable copies of all of its Transactional Records of UMAX's dealings with Micro Center during the entire period of January 1, 1996 through November 30, 2004.

The Master shall proceed with all reasonable diligence in the investigation and reporting of these matters, and may communicate *ex parte* with the parties and their counsel in pursuing his investigation, but may not receive any additional or new documents from any party unless all parties receive such records and documents at the same time.

The Master shall use his best efforts to complete his work and submit his report by February 1, 2005. The materials received by the Master shall be preserved by the Master and, filed with the Court at the time the Master files his report with the Court and serves a copy of his report upon all counsel in this case.

The Master may compel the parties, their employees and representatives to give evidence and produce data and records at any hearings or other proceedings conducted by the Master, and is authorized to issue subpoenas and subpoenas *duces tecum* for these purposes. The Master may recommend a contempt sanction against a party or non-party and such other sanctions as he determines to be appropriate.

To the extent there arise any disputes concerning the furnishing of access to UMAX's Computer Systems, databases, and/or data in this case, such disputes shall be first presented to Peter Vogel as Special Master who shall have the full and complete authority to resolve such disputes, subject only to further Order of this Court. The parties will comply with the instructions and directives of the Special Master until further Order of this Court with regard to the matters referred to the Master, as described above, and where necessary the Master may

Appendix

conduct hearings and compel the production before him of evidence and witnesses. The Master is further empowered to take all measures necessary and proper for the efficient performance of his duties, to regulate all proceedings before the Master, examine witnesses and evidence, engage the assistance of clerical and other help, and take other measures necessary or proper for the efficient performance of his duties.

The Master shall not, and is not authorized to, make any legal rulings, determine the admissibility of any evidence, or admit or exclude any evidence from proceedings before him, adjudicate anyone in contempt for failing to comply with his orders, or make any legal rulings on the issues raised in the Discovery Motions; all of which rights, powers and duties are retained by and reserved for the Court.

The Special Master shall investigate these matters described above and submit a written report to the Court and parties describing the results of his investigation and make recommendations to the Court, as appropriate.

Thereafter the Court, which has taken the matters held in abeyance at the hearing on Micro Center's First Set of Discovery Motions, and those matters argued at the hearing on Plaintiff's Second Set of Discovery Motions, under advisement, will review and consider the Master's report, any additional evidence or argument of counsel, may refer additional matters to the Master, and thereafter decide the matters raised in the Discovery Motions.

ORDERED THIS _____ of _____, 2004

JUDGE W. BRUCE WOODY

AGREED AND APPROVED AS TO SUBSTANCE AND FORM:

STEPHEN KAPLAN, P.C.

BROWNING & FLEISHMAN, P.C.

STEPHEN E. KAPLAN State Bar No.11095200 7557 Rambler Road, Suite 700 Dallas, Texas 75231 214.346.6048 – Telephone 214.346.6049 – Facsimile

ATTORNEYS FOR PLAINTIFF

JOHN G. BROWNING State Bar No. 03223050 701 Commerce Street, Suite 510 Dallas, Texas 75202 214.752.4130 – Telephone 214.227.9010 – Facsimile

ATTORNEYS FOR DEFENDANT


Chapter 18

Authentication and Admissibility

Judge Karl E. Hays and Paul M. Leopold

§ 18.1 Introduction

In 1999, former U.S. District Judge Samuel Kent offered the following thoughts on the reliability of what he referred to as "voodoo information taken from the Internet":

While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No website is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content of any website from any location at any time.¹

In the early days of computers, this mistrust of technology led one appellate court to express the view that proof of the reliability of the computer generating the business records at issue was necessary to establish the proper predicate for the admission of printouts obtained from the computer.²

Today, however, most courts share the view that the standards and procedures for admitting electronically stored information ("ESI") are no different than the standards and procedures employed in admitting traditional evidence.

For example, in addressing the question of what was necessary to authenticate transcripts of instant message conversations, a Pennsylvania appellate court opined:

^{1.} St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999).

^{2.} R.R. Comm'n v. S. Pac. Co., 468 S.W.2d 125, 129 (Tex. App.-Austin 1971, writ ref'd n.r.e.).

Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. The argument is that e-mails or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. Unless the purported author is actually witnessed sending the e-mail, there is always the possibility it is not from whom it claims. As appellant correctly points out, anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that email messages and similar forms of electronic communication can be properly authenticated within the existing framework of [the rules of evidence and case law]. We see no justification for constructing unique rules of admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.³

If the procedures for admitting ESI are no different than those governing the admission of nonelectronic traditional evidence, exactly what does it take to insure the admission of ESI? This question was perhaps most appropriately answered by Chief United States Magistrate Judge Paul W. Grimm in his seminal memorandum opinion in *Lorraine v. Markel American Insurance Company*:

Whether ESI is admissible into evidence is determined by a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible. Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI relevant as determined by rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it authentic as required by rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it hearsay as defined by rule 801, and if so, is it covered by an applicable exception (rules 803, 804 and 807); (4) is

^{3.} In re F.P., 878 A.2d 91, 95–96 (Pa. Super. Ct. 2005) (citation omitted).

the form of the ESI that is being offered as evidence an original or duplicate under the original writing rule, or if not, is there admissible secondary evidence to prove the content of the ESI (rules 1001–1008); and (5) is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or one of the other factors identified by rule 403, such that it should be excluded despite its relevance.⁴

While issues regarding ESI often center on questions of authentication and concerns about reliability, attorneys should nct overlook each of the "evidentiary hurdles" noted by Judge Grimm. For example, in *Segovia v State*,⁵ the defendant sought to introduce digital photographs of the crime scene that were taken shortly before trial. Although the photos had been properly authenticated, the court held that it was proper to exclude them on the grounds of relevancy because they were not taken at the time the crime occurred and therefore did not accurately depict the crime scene as it was at the time the crime was committed.

§ 18.2 Authentication

The requirement of authentication or identification is a condition precedent to admissibility. Evidence is not even relevant if it is not authentic.⁶ This requirement is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.⁷ Unless the evidence sought to be admitted is self-authenticating under Texas Rule of Evidence 902 or Texas Rule of Civil Procedure 193.7, extrinsic evidence must be adduced prior to its admission. Rule 901(b) of the Texas Rules of Evidence contains a nonexclusive list of illustrations of methods of authentication that comply with the rule.

A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be. As stated in *United States v. Goichman*, "[w]hat appellant overlooks is that the showing of authenticity is not on a par with the more technical evidentiary rules, such as hearsay exceptions, governing admissibility. Rather, there need be only a prima facie showing, to the court, of authenticity, not a full argument on admissibility."⁸

- 7. Tex. R. Evid. 901.
- 8. United States v. Goichman, 547 F.2d 778, 784 (3d Cir. 1976).

^{4.} Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007) (mem. op.) (emphasis in original).

^{5. 467} S.W.3d 545, 550-51 (Tex. App.—San Antonio 2015, pet. ref'd).

^{6.} Tienda v. State, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012).

This is not a particularly high barrier to overcome. For example, in *United States v. Safavian*, the court analyzed the admissibility of several e-mails, noting—

[t]he question for the court under rule 901 is whether the proponent of the evidence has "offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is." The court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so.⁹

The authentication requirements of Texas Rule of Evidence 901 are designed to set up a threshold preliminary standard to test the reliability of evidence, subject to later review by an opponent's cross-examination.

Determining what degree of foundation is appropriate in any given case is in the judgment of the court. The required foundation will vary not only with the particular circumstances but also with the individual judge.

Obviously, there is no "one size fits all" approach that can be taken when authenticating electronic evidence, in part because technology changes so rapidly that it is often new to many judges. But as it continues to change, evidentiary principles from current or past technology can continue to be applied.¹⁰

§ 18.2:1 Tienda v. State

Any examination of the issues surrounding the authentication of ESI in Texas courts should begin with a careful reading of the Texas Court of Criminal Appeals' opinion in *Tienda v. State.*¹¹ In that case, the State had introduced, at trial, printouts of a MyS-pace profile allegedly belonging to the defendant and implicating him in a shooting. The issue of whether the MySpace pages were sufficiently authenticated by circumstantial evidence was appealed to the Texas Court of Criminal Appeals, which addressed the issue very specifically:

^{9.} United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006) (quoting 5 Fed. R. Evid. Manual § 901.02[1] at 901-5-901-6).

^{10.} See, e.g., Price v. State, No. 01-17-00717-CR, 2019 WL 1186664, at *6–7 (Tex. App.—Dallas Mar. 14, 2019, no pet.) (mem. op., not designated for publication) (comparing Kik app messages with text messages); Norris v. State, No. 06-16-00150-CR, 2017 WL 1536198, at *1, n.2 (Tex. App.—Texarkana Apr. 27, 2017, pet. ref'd) (mem. op., not designated for publication) (comparing Facebook Messenger messages with e-mail and text messages).

^{11.} Tienda, 358 S.W.3d 633.

Rule 901(a) of the Rules of Evidence defines authentication as a "condition precedent" to admissibility of evidence that requires the proponent to make a threshold showing that would be "sufficient to support a finding that the matter in question is what its proponent claims." Whether the proponent has crossed this threshold as required by rule 901 is one of the preliminary questions of admissibility contemplated by rule 104(a). The trial court should admit proffered evidence "upon, or subject to the introduction of evidence sufficient to suppor: a finding of" authenticity. The ultimate question whether an item of evidence is what its proponent claims then becomes a question for the fact finder—the jury, in a jury trial. In performing its rule 104 gate-keeping function, the trial court itself need not be persuaded that the proffered evidence is authentic. The preliminary question for the trial court to decide is simply whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable jury determination that the evidence he has proffered is authentic.¹²

The court continued by noting that there is no specific procedure for authenticating electronic evidence; rather the means of authentication will depend on the facts of the case:

Evidence may be authenticated in a number of ways, including by direct testimony from a witness with personal knowledge, by comparison with other authenticated evidence, or by circumstantial evidence. Courts and legal commentators have reached a virtual consensus that, although rapidly developing electronic communications technology often presents new and protean issues with respect to the admissibility of electronically generated, transmitted and/or stored information, including information found on social networking websites, the rules of evidence already in place for determining authenticity are at least generally "adequate to the task." Widely regarded as the watershed opinion with respect to the admissibility of various forms of electronically stored and/or transmitted information is Lorraine v. Markel American Insurance Co. There the federal magistrate judge observed that "any serious consideration of the requirement to authenticate electronic evidence needs to acknowledge that, given the wide diversity of such evidence, there is no single approach to authentication that will work in all instances." Rather, as with the authentication of any kind of proffered evidence, the best or most appropriate method for

^{12.} Tienda, 358 S.W.3d at 638 (internal citations omitted).

authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case.¹³

The *Tienda* court went on to note how other jurisdictions have addressed the issue of authenticating ESI:

Like our own courts of appeals here in Texas, jurisdictions across the country have recognized that electronic evidence may be authenticated in a number of different ways consistent with federal rule 901 and its various state analogs. Printouts of e-mails, Internet chat room dialogs, and cellular phone text messages have all been admitted into evidence when found to be sufficiently linked to the purported author so as to justify submission to the jury for its ultimate determination of authenticity. Such prima facie authentication has taken various forms. In some cases, the purported sender actually admitted to authorship, either in whole or in part, or was seen composing it. In others, the business records of an internet service provider or a cell phone company have shown that the message originated with the purported sender's personal computer or cell phone under circumstances in which it is reasonable to believe that only the purported sender would have had access to the computer or cell phone. Sometimes the communication has contained information that only the purported sender could be expected to know. Sometimes the purported sender has responded to an exchange of electronic communications in such a way as to indicate circumstantially that he was in fact the author of the particular communication, the authentication of which is in issue. And sometimes other circumstances, peculiar to the facts of the particular case, have sufficed to establish at least a prima facie showing of authentication.¹⁴

In particular, the *Tienda* court specifically examined the merits of *Griffin v. State*, a Maryland intermediate appellate court opinion:

[T]he Maryland Court of Appeals recognized that such postings may readily be authenticated, explicitly identifying three nonexclusive methods. First, the proponent could present the testimony of a witness with knowledge; or, in other words, "ask the purported creator if she indeed created the profile and also if she added the posting in question." That may not be possible where, as here, the State offers the evidence to be authenticated

^{13.} Tienda, 358 S.W.3d at 638–39 (internal citations omitted).

^{14.} Tienda, 358 S.W.3d at 639-41.

and the purported author is the defendant. Second, the proponent could offer the results of an examination of the Internet history or hard drive of the person who is claimed to have created the profile in question to determine whether that person's personal computer was used to originate the evidence at issue. Or, third, the proponent could produce information that would link the profile to the alleged person from the appropriate employee of the social networking website corporation.¹⁵

The *Tienda* court also acknowledged that some courts have held electronic evidence to a higher standard of authentication than other forms of evidence:

However, mindful that the provenance of such electronic writings can sometimes be open to question—computers can be hacked, protected passwords can be compromised, and cell phones can be purloined—courts in other cases have held that not even the prima facie demonstration required to submit the issue of authentication to the jury has been satisfied. That an e-mail on its face purports to come from a certain person's e-mail address, that the respondent in an internet chat room dialog purports to identify himself, or that a text message emanates from a cell phone number assigned to the purported author—none of these circumstances, without more, has typically been regarded as sufficient to support a finding of authenticity.¹⁶

In the *Tienda* case, the Texas Court of Criminal Appeals found that the State presented sufficient circumstantial evidence to authenticate the MySpace pages and postings as those of the defendant:

This combination of facts—(1) the numerous photographs of the appellant with his unique arm, body, and neck tattoos, as well as his distinctive eyeglasses and earring; (2) the reference to [the victim's] death and the music from his funeral; (3) the references to the appellant's . . . gang; and (4) the messages referring to . . . the [MySpace] user having been on a monitor for a year (coupled with the photograph of the appellant lounging in a chair displaying an ankle monitor) sent from the MySpace pages . . . is sufficient to support a finding by a rational jury that the MySpace pages that the State offered into evidence were created by the appellant. This is ample circumstantial evidence—taken as a whole with all of the individual, particular

^{15.} Tienda, 358 S.W.3d at 647.

^{16.} Tienda, 358 S.W.3d at 641–42.

details considered in combination—to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them.¹⁷

While the court acknowledged the possibility that someone could have forged the pages to set up the defendant, it held that that issue was one for the fact finder, not for the court as prerequisite to authentication:

It is, of course, within the realm of possibility that the appellant was the victim of some elaborate and ongoing conspiracy. Conceivably some unknown malefactors somehow stole the appellant's numerous self-portrait photographs, concocted boastful messages about [the victim's] murder and the circumstances of that shooting, was aware of the music played at [the victim's] funeral, knew when the appellant was released on pretrial bond with electronic monitoring and referred to that year-long event along with stealing the photograph of the grinning appellant lounging in his chair while wearing his ankle monitor. But that is an alternate scenario whose likelihood and weight the jury was entitled to assess once the State had produced a prima facie showing that it was the appellant, not some unidentified conspirators or fraud artists, who created and maintained these My-Space pages.¹⁸

§ 18.2:2 Self-Authentication: Federal and Texas Rule of Evidence 902

Rule 902 of the Federal and Texas Rules of Evidence specifically provide that extrinsic evidence of authenticity as a prerequisite to admissibility is not required with respect to the types of documents specifically enumerated in those rules. Of particular note, with respect to ESI, are 902(5) Official Publications and 902(6) Newspapers and Periodicals. Several Texas cases have held that documents printed out from an official federal, state, or local government-run website are self-authenticating.¹⁹ In fact, because they are self-authenticating, it is proper for a court to take judicial notice of them.²⁰ The same should also be true for pages downloaded from websites such as

^{17.} Tienda, 358 S.W.3d at 645.

^{18.} Tienda, 358 S.W.3d at 645-46.

^{19.} See In re Doe, 501 S.W.3d 313, 321 n.11 (Tex. App.—Houston [14th Dist.] 2016, no pet.); Avery v. LPP Mortgage, Ltd., No. 01-14-01007-CV, 2015 WL 6550774, at *3 (Tex. App.—Houston [1st Dist.] Oct. 29, 2015, no pet.) (mem. op.); Williams Farms Produce Sales, Inc. v. R&G Produce Co., 443 S.W.3d 250, 259 (Tex. App.—Corpus Christi–Edinburg 2014, no pet.).

^{20.} In re Doe, 501 S.W.3d at 321 n.11; see Tex. R. Evid. 204.

§ 18.2:3 Self-Authentication: Texas Rule of Civil Procedure 193.7

Rule 193.7 of the Texas Rules of Civil Procedure provides that documents produced in response to written discovery are automatically authenticated against the producing party for use in any pretrial proceeding or at trial, unless the producing party objects to the authenticity within ten days of receiving notice that the document will be used.²¹ A party, however, cannot simply produce a document to the opposing party to make that document self-authenticating.²²

§ 18.2:4 Self-Authentication: Federal Court Local Rules

There is no parallel Federal Rule of Civil Procedure to Tex. R. Civ. P. 193.7. However, many federal district courts have adopted a provision similar to the following:

Authentication of Documents. A party's production of a document in response to written discovery authenticates the document for use against that party in any pretrial proceeding or at trial unless not later than fourteen days or a period ordered by the court or specified by rule CV-16(e), after the producing party has actual notice that the document will be used—the party objects to the authenticity of the document, or any part of it, stating the specific basis for objection. An objection must be either on the record or in writing and must have a good faith factual and legal basis. An objection made to the authenticity of only part of a document does not affect the authenticity of the remainder. If objection is made, the party attempting to use the document should be given a reasonable opportunity to establish its authenticity.²³

23. Western District of Texas, Local Rule CV-26.

§ 18.2

^{21.} Tex. R. Civ. P. 193.7; Blanche v. First Nationwide Mortg. Corp., 74 S.W.3d 444, 451 (Tex. App.-Dallas 2002, no pet.).

^{22.} Tex. Black Iron, Inc. v. Arawak Energy Int'l Ltd., 566 S.W.3d 801, 812–13 (Tex. App.—Houston [14th Dist.] 2018, pet. denied).

§ 18.2:5 Self-Authentication: The Reply-Letter Doctrine

"It is an accepted rule of evidence that a letter received in due course through the mails in response to a letter sent by the receiver is presumed to be the letter of the person whose name is signed to it and is thus self-authenticating."²⁴ But the original letter must still be authenticated under traditional rules.²⁵ Texas courts have applied this same rule to electronic communications, including e-mails and text messages, although some courts have held that it is a rule of admissibility under 901, rather than a self-authenticating rule.²⁶

§ 18.2:6 Self-Authentication: Relevant Case Law Regarding Self-Authentication

In re Doe

A statute required a doctor to furnish a government-produced booklet to a minor seeking judicial bypass of parental consent for an abortion. The Texas court of appeals explained that it was therefore reasonable to conclude that the minor received the booklet. The booklet was self-authenticating, and the court could take judicial notice of the booklet.²⁷

Avery v. LPP Mortgage

The court held that printouts from the Federal Deposit Insurance Corporation (FDIC) website are self-authenticating in a summary judgment proceeding.²⁸

Williams Farms Produce Sales, Inc. v. R&G Produce Co.

A seller obtained a turnover order for all assets of a buyer, including a cause of action. The buyer argued that an LLC by a similar name, not the corporation in this suit,

^{24.} United States v. Wolfson, 322 F. Supp. 798, 812 (D. Del. 1971), aff^{*}d, 454 F.2d 60 (3d Cir. 1972) (citing Scofield v. Parlin & Orendorff Co., 61 F. 804, 806 (7th Cir. 1894)); accord Black v. Callahan, 876 F. Supp. 131, 132 (N.D. Tex. 1995), aff^{*}d, 79 F.3d 1143 (5th Cir. 1996) (citing United States v. Weinstein, 762 F.2d 1522 (11th Cir.), opinion modified on denial of reh^{*}g, 778 F.2d 673 (11th Cir. 1985)).

^{25.} United States v. Wolfson, 322 F. Supp. at 812.

^{26.} See Butler v. State, 459 S.W.3d 595, 602 n.6 (Tex. Crim. App. 2015) (text messages, letters, emails, instant messages, "and other similar written forms of communications"); *Manuel v. State*, 357 S.W.3d 66, 75 (Tex. App.—Tyler 2011, pet. ref'd) (text messages); *Varkonyi v. State*, 276 S.W.3d 27, 35 (Tex. App.—El Paso 2008, pet. ref'd) (e-mails).

^{27.} In re Doe, 501 S.W.3d 313, 321 n.11 (Tex. App.-Houston [14th Dist.] 2016).

^{28.} Avery, 2015 WL 6550774, at *3.

Authentication and Admissibility

Murray v. State

The State, in seeking to convict the defendant of compelling prostitution, introduced pictures, private messages, and other electronic data from a Facebook account assigned to the defendant, by way of a "Certificate of Authenticity of Domestic Records of Regularly Conducted Activity" executed by Facebook's Records Custodian. The court held that the certificate complied with rule 902(10)'s business records affidavit requirements, and thus the Facebook evidence was self-authenticating. The opinion does not explain how the State obtained the certificate from Facebook.³⁰

People v. Pierre

In this New York case, the court held that the reply-letter doctrine applied to instant messages, where the person sent an instant message to a screen name and received a reply. The content in the reply supported the conclusion that the message was sent by defendant, and no evidence was admitted to show that anyone else had motive or opportunity to impersonate defendant by using his screen name.³¹

§ 18.2:7 Authenticating E-Mail

There are many ways in which e-mail evidence may be authenticated. An e-mail is properly authenticated if its appearance, contents, substance, or other distinctive characteristics, taken in conjunction with circumstances, support a finding that the document is what its proponent claims.³² As noted by Judge Grimm in his opinion in the Lorraine case, "[e]-mail messages may be authenticated by direct or circumstantial evidence. An e-mail message's distinctive characteristics, including its 'contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances' may be sufficient for authentication."³³

33. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007) (mem. op.).

§ 18.2

^{29.} Williams Farms Produce Sales, Inc. v. R&G Produce Co., 443 S.W.3d 250, 259 (Tex. App.-Corpus Christi-Edinburg 2014).

^{30.} Murray v. State, 534 S.W.3d 540, 545 (Tex. App.-San Antonio 2017, no pet.).

^{31.} People v. Pierre, 838 N.Y.S.2d 546, 548-49 (N.Y. App. Div. 2007).

^{32.} Manuel v. State, 357 S.W.3d 66, 76-77 (Tex. App.-Tyler 2011, pet. denied).

Printouts of e-mail messages ordinarily bear the sender's e-mail address, providing circumstantial evidence that the message was transmitted by the person identified in the e-mail address. In responding to an e-mail message, the person receiving the message may transmit the reply using the computer's reply function, which automatically routes the message to the address from which the original message came. Use of the reply function indicates that the reply message was sent to the sender's listed e-mail address.

The contents of the e-mail may help show authentication by revealing details known only to the sender and the person receiving the message. However, the sending address in an e-mail message is not conclusive, since e-mail messages can be sent by persons other than the named sender. For example, a person with unauthorized access to a computer can transmit e-mail messages under the computer owner's name. Because of the potential for unauthorized transmission of e-mail messages, authentication requires testimony from a person with personal knowledge of the transmission or receipt to ensure its trustworthiness.³⁴

§ 18.2:8 Relevant Case Law Regarding Authenticating E-Mails

United States v. Siddiqui

E-mail may be authenticated entirely by circumstantial evidence, including its distinctive characteristics.³⁵

United States v. Safavian

This case recognized that e-mail may be authenticated by distinctive characteristics under Federal Rule of Evidence 901(b)(4) or by comparison of exemplars with other e-mails that already have been authenticated under rule 901(b)(3).³⁶

Rambus, Inc. v. Infineon Techs, AG

E-mail that qualifies as business record may be self-authenticating under Federal Rule of Evidence 902(11).³⁷

37. Rambus, Inc. v. Infineon Techs, AG, 348 F. Supp. 2d 698, 707 (E.D. Va. 2004).

^{34.} Lorraine, 241 F.R.D. at 554-55.

^{35.} United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000).

^{36.} United States v. Safavian, 435 F. Supp. 2d at 40.

In re F.P.

E-mail may be authenticated by direct or circumstantial evidence.³⁸

Shea v. State

An e-mail can be authenticated by testimony that the witness was familiar with the sender's e-mail address and that she had received the e-mails in question from him.³⁹

Massimo v. State

Another court enumerated several characteristics to consider when determining whether an e-mail has been properly authenticated, including:

- 1. consistency with the e-mail address on another e-mail sent by the defendant;
- 2. the author's awareness through the e-mail of the details of defendant's conduct;
- 3. the e-mail's inclusion of similar requests that the defendant had made by phone during the time period; and
- 4. the e-mail's reference to the author by the defendant's nickname.⁴⁰

Manuel v. State

An e-mail is sufficiently authenticated when a person responds to an e-mail that was sent to the person's e-mail address.⁴¹

Martinez, v. AA Foundries, Inc.

Cartoons and e-mails laid on a desk cannot be properly authenticated by simply stating that they must have come from the defendant as that person was the only one to have access to the desk.⁴² This is akin to an e-mail on its face purporting to come from the purported author, without other distinct characteristics, usually not being sufficient to show authenticity.⁴³

- 39. Shea v. State, 167 S.W.3d 98, 105 (Tex. App.-Waco 2005, pet. ref'd).
- 40. Massimo v. State, 144 S.W.3d 210, 215 (Tex. App.-Fort Worth 2004, no pet.).
- 41. Manuel v. State, 357 S.W.3d 66, 76-77 (Tex. App.-Tyler 2011).

42. Martinez v. AA Foundries, Inc., No. 04-11-00879-CV, 2013 WL 346814 at *5 (Tex. App.—San Antonio Jan. 30, 2013, no pet.) (mem. op.).

^{38.} In re F.P., 2005 PA Super 220, 878 A.2d 91 (2005)

Sennett v. State

E-mail authenticated through witness testimony that the appellant's e-mail address had always been the same; that the witness was familiar with the e-mail address; and before the sexual assault, the subject of the appeal, the appellant told the witness that she was "beautiful" and then referred to her the same way in an e-mail response to the witness's e-mail to Appellant.⁴⁴ Further, the e-mails contained content that only the appellant and the witness would have known.

St. Angelo v. State

The defendant was convicted of murder. The victim had received several threatening e-mails from the defendant and had forwarded the e-mails to her boss. At trial, the State introduced the forwarded e-mails through the victim's boss. The victim's boss testified that she received the e-mails to her e-mail address from the victim's e-mail address and that the victim had represented that the forwarded e-mails were from the defendant. The witness also testified that the string of e-mails fairly and accurately represented what the victim had sent to her. Additionally, one of the e-mails referred to the victim's electronic signature, her business address, and business phone numbers. The court held that these facts were sufficient to authenticate the forwarded e-mails.⁴⁵

State v. Robinson

The State offered emails between the defendant and his victims to establish its theory of the case. Instead of offering copies of the original e-mails, the State offered redacted copies of the e-mails obtained from law enforcement. The State redacted the part of the e-mails that showed they had been forwarded to law enforcement. The court of appeals held that, because defendant had received unredacted copies during discovery and the original recipient testified that the redacted copies were true and accurate copies of the e-mails on the original computer, the e-mails were properly authenticated. The court also noted that any deviations in the e-mails went to the weight of the evidence, rather than admissibility.⁴⁶

^{43.} Martinez, 2013 WL 346814, at *5.

^{44.} Sennett v. State, 406 S.W.3d 661, 669 (Tex. App.-Eastland April 25, 2013, no pet.).

^{45.} St. Angelo v. State, No. 02-15-00107-CR, 2016 WL 1393387 (Tex. App.—Fort Worth Apr. 7, 2016, pet. ref'd) (mem. op., not designated for publication).

§ 18.2:9 Relevant Case Law Regarding Authenticating Text Messages

Text messages can be authenticated by applying the same factors as e-mails.⁴⁷

Montoya v. State

The defendant argued that the state failed to authenticate a text message because the witness did not see the text message arrive from the defendant's phone, nor could the witness testify the texts were sent by the defendant's recognizable telephone number.⁴⁸ The court held that the witness testified he knew when his mother received text messages from the defendant. Because he was better with technology, he saved the texts on the phone. The witness then pulled out his mother's phone and pulled up the text message for the attorneys to review. The court held that "[g]iven the low threshold for authentication under rule 901(b)(1), we conclude [the witness's] testimony was sufficient that a reasonable fact fir.der could properly determine that the text message was what it claimed to be—a text message from [the defendant]."

Gardner v. State

A witness was permitted to testify about the contents of text messages the victim received from the accused and the emotional effect the texts had on the victim.⁴⁹

Franklin v. State

The defendant complained that the State failed to properly authenticate text messages from a cellular phone.⁵⁰ On appeal, the court held that there was sufficient evidence of authentication, finding that—

Evidence was presented that the defendant had a cell phone in his hand when the police stopped him;

^{46.} State v. Robinson, 363 P.3d 875, 1024–26 (2015), disapproved of by State v. Cheever, 306 Kan. 760, 402 P.3d 1126 (2017), disapproved on other grounds, State v. Cheever, 306 Kan. 760, 402 P.3d 1126, cert. denied, 138 S. Ct. 560, 199 L. Ed. 2d 441 (2017), and abrogated by State v. Boothby, 448 P.3d 416 (Kan. 2019).

^{47.} Manuel v. State, 357 S.W.3d 66, 76-77 (Tex. App.-Tyler 2011).

^{48.} Montoya v. State, No. 05-10-01468-CR, 2012 WL 1059699, at *2-3 (Tex. App.—Dallas Mar. 30, 2012) (mem. op.).

^{49.} Gardner v. State, 306 S.W.3d 274, 287 (Tex. Crim. App. 2009).

^{50.} Franklin v. State, No. 05-11-00990-CR, 2012 WL 4801522, at *6-7 (Tex. App.—Dallas Oct. 10, 2012, no pet.) (not designated for publication).

The same cell phone was taken from him when he was arrested;

A forensic search of the same phone retrieved contacts, call histories, and text messages; and

The text messages from that phone referenced "the bridge," where the accomplices lived, and were sent on or at the time of the crime.⁵¹

Although the State could not prove that the defendant sent or received the messages, the evidence was such for the fact finder to find that the defendant did send and receive the messages.⁵²

Joseph v. State

The appellant's verbal messages to witnesses were so similar to the purported texts that they could be properly authenticated as coming from the appellant.⁵³

Butler v. State

The defendant was convicted for aggravated kidnapping. A week prior to trial, the defendant called and texted the victim. The Texas Court of Criminal Appeals held that the content and context of the text messages themselves constituted circumstantial evidence of the authenticity of the messages. In addition to exchanging texts, the fact that the defendant actually called the victim during the time period when the text messages were being exchanged adds additional circumstantial evidence. The court further explained that rational inferences existed, from the context of the messages, that defendant authored them. The court also held that, although the victim had been impeached, rule 901 does not require that the trial court determine the credibility of the evidence to establish authenticity. Further, it does not require, as a condition of admissibility, that the "witness with knowledge' is necessarily worthy of belief."⁵⁴

§ 18.2:10 Authenticating Internet Website Postings

When determining the admissibility of exhibits containing representations of the contents of website postings of a party, "the issues that have concerned courts include the

^{51.} Franklin, 2012 WL 4801522, at *6.

^{52.} Franklin, 2012 WL 4801522, at *6.

^{53.} Joseph v. State, No. 14-11-00776-CR, 2013 WL 2149779, at *3 (Tex. App.—Houston [14th Dist.] May 16, 2013, no pet.) (mem. op.).

^{54.} Butler v. State, 459 S.W.3d 595, 603-05 (Tex. Crim. App. 2015).

possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting."⁵⁵

The Lorraine court offered additional valuable insight for admitting website postings:

One commentator has observed, "[i]n applying [the authentication standard] to website evidence, there are three questions that must be answered explicitly or implicitly. (1) What was actually on the website? (2) Does the exhibit or testimony accurately reflect it? (3) If so, is it attributable to the owner of the site?

The same author suggests that the following factors will influence courts in ruling whether to admit evidence of internet postings:

The length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g., financial information from corporations); whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; whether the data has been republished by others who identify the source of the data as the website in question?

Counsel attempting to authenticate exhibits containing information from Internet websites need to address these concerns in deciding what method of authentication to use, and the facts to include in the foundation.⁵⁶

The authentication rules most likely to apply, singly or in combination, are:

- 901(b)(1) (witness with personal knowledge);
- 901(b)(3) (expert testimony);
- 901(b)(4) (distinctive characteristics);
- 901(b)(7) (public records);

^{55.} Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 555 (D. Md. 2007).

^{56.} Lorraine, 241 F.R.D. at 555 (quoting Gregory P. Joseph, Internet and Email Evidence, 13 Prac. Litigator (Mar. 2002), reprinted in 5 Stephen A Saltzburg, Michael M. Martin, and Daniel J. Capra, Federal Rules of Evidence Manual, Part 4 at 22 (9th ed. 2006))

- 901(b)(9) (system or process capable of producing a reliable result); and
- 902(5) (official publications).

§ 18.2:11 Relevant Case Law Regarding Authenticating Internet Website Postings

United States v. Jackson

The trial court properly excluded evidence of website postings because proponent failed to show that the sponsoring organization actually posted the statements, as opposed to a third party.⁵⁷

St. Luke's Cataract and Laser Inst., P.A. v. Sanderson

The plaintiff failed to authenticate exhibits of the defendant's website postings because affidavits used to authenticate the exhibits were factually inaccurate and the author lacked personal knowledge of the website.⁵⁸

Musgrove v. State

One case addressed an online personal ad and found that it was not necessary for authentication to show that the person placed the ad, only that the exhibit was an authentic copy of the actual online ad.⁵⁹ Whether the party placed the ad did not go to the authenticity of the exhibit, but rather to the underlying issues in the case.

§ 18.2:12 Relevant Case Law Regarding Facebook Postings/Social Networking

State v. Eleck

Showing that messages came from a particular Facebook account insufficient to authenticate messages without further "foundational proof."⁶⁰

^{57.} United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000).

^{58.} St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, No. 8:06-CV-223-T-MSS, 2006 WL 1320242, at *2 (M.D. Fla. May 12, 2006).

^{59.} *Musgrove v. State*, No. 03-09-00163-CR, 2009 WL 3926289, at *2 (Tex. App.—Austin Nov. 20, 2009, no pet.) (mem. op., not designated for publication).

^{60.} State v. Eleck, 23 A.3d 818, 824 (Conn. App. 2011), aff'd on other grounds, 100 A.3d 817 (2014).

Commonwealth v. Purdy

Holding that e-mail sent from Facebook account bearing defendant's name not sufficiently authenticated without additional "confirming circumstances."⁶¹

Campbell v. State

Like e-mail messages under the holding in *Massimo v. State*, Facebook messages may also be authenticated by internal characteristics, such as the speech pattern of the purported author, the fact that the messages reference specifics about an incident or occurrence between the parties, as well as circumstantial evidence regarding the parties' access to the Facebook account. For example, in this case, the only two parties that had access to the account were the victim and the defendant, the defendant admitted he had a Facebook account, and the victim admitted to receiving messages from the defendant's Facebook account.⁶²

Rene v. State

The Fourteenth District Court of Appeals considered the defendant's MySpace relevant to a criminal case.⁶³ The court applying *Tienda*, held that, although there was less circumstantial evidence to link the MySpace page to the defendant, as in *Tienda*, there was still some:

Testimony by a witness that the MySpace page was discovered by online search of the defendant's name;

Headings at the top of the page stating "137's Don Lo," the defendant's gang number and name;

Witness testimony that the defendant used the nickname "Lo";

The defendant appeared in almost all the photographs on the profile; and

The defendant's distinctive tattocs could be seen in the photographs on the profile, especially photographs of children on his arms later matched to photographs of his children by witness testimony.⁶⁴

^{61.} Com. v. Purdy, 945 N.E.2d 372, 380-82 (Mass. 2011).

^{62.} Campbell v. State, 382 S.W.3d 545, 551-52 (Tex. App.-Austin 2012, no pet.).

^{63.} Rene v. State, 376 S.W.3d 302, 303 (Tex. App.-Houston [14th Dist.] 2012, pet. denied).

^{64.} Rene, 376 S.W.3d at 307.

As a result, there was sufficient circumstantial evidence to authenticate the MySpace page as the defendant's.⁶⁵

Bullman v. State

The State obtained Facebook records from the defendant that contained several exchanges between the defendant and the minor victim. The court explained that while the messages, on their face, were sent from an account bearing the defendant's name, that fact alone was not sufficient to authenticate the messages without more. The messages were properly authenticated when the victim testified that she had received the messages from a Facebook account bearing the defendant's name, that she knew she was communicating with the defendant because of the way he said things, and that they communicated about things only she and the defendant would know about. For example, the defendant created a code and required the victim to use the code whenever they communicated. A forensics investigator also testified that he was able to determine that the account had been logged into from different locations outside of Texas where the defendant had travelled and that the account was connected with the defendant's e-mail address and phone number.⁶⁶

Coe v. State

The defendant and the minor victim had known each other and had been friends on Facebook. The victim said that the defendant made her feel awkward when he commented on one of her pictures that she "looked cute," so the victim's sister started monitoring her Facebook account. The victim's sister, posing as the victim, initiated a Facebook chat with the defendant, who gave her his cell phone number. The following day, the victim's sister, again posing as the victim, sent a text message to the defendant, and a conversation ensued, wherein the defendant made several sexually suggestive remarks. The defendant asked for nude pictures of the victim, and her sister sent random pictures she found online. The defendant responded with nude pictures of himself. An FBI agent eventually took over posing as the victim and continued messaging the defendant through Facebook and also Google Chat and email. The FBI agent, still posing as the victim, arranged a rendezvous with the defendant to have sex, and when the defendant arrived, the agent arrested him. Photographs of the messages were admitted against an authenticity objection. The court of appeals held that the messages were properly authenticated because the victim's sister identi-

^{65.} Rene, 376 S.W.3d at 307.

^{66.} Bullman v. State, No. 09-14-00196-CR, 2016 WL 1469592, at *5-7 (Tex. App.—Beaumont Apr. 13, 2016, no pet.) (mem. op., not designated for publication).

Authentication and Admissibility

fied the photographs and testified that she had taken them. The victim's sister also identified the text messages exchanged between her and the cell phone number that the defendant had given through Facebook. The FBI agent testified that that cell phone number did indeed belong to the defendant and that the defendant arrived at the designated time and place referenced in the messages, and announced his arrival using the same cell phone number.⁶⁷

Dering v. State

At a hearing on a motion to change venue, the defendant sought to introduce dozens of Facebook posts by third parties to show that, because of media coverage, the defendant could not get a fair trial in the county where his case was filed. The posts were not made on the defendant's Facebook account. The sponsoring witness was not the owner of any of the posting accounts or the account to which any posts were posted. The court of appeals held that, because the Facebook posts that were admitted into evidence were posted by unavailable third parties, not by the defendant, and because the sponsoring witness could only identify some of the posters but could not testify whether they were the ones who actually made the posts, the Facebook posts were not sufficiently authenticated.⁶⁸

R.Z. v. Tex. Dep't of Family & Protective Servs.

The department offered printouts from an adult dating website that contained pictures of the respondent, identified her by a different name, and stated that she was a female escort. The evidence also included a phone number, e-mail address, and cost of services. The respondent objected on the grounds that the evidence had not been properly authenticated. She did not dispute that the pages were posted on the website, that the photographs were of her, or that the e-mail address was hers. Instead, she argued that certain information about her was incorrect, including her height and phone number. A witness from the department testified that the phone number listed on the site was what the department had had on file for the respondent for several months. Furthermore, Facebook pages were admitted, without objection, that showed that the evidence was sufficient to properly authenticate the website printouts.⁶⁹

^{67.} Coe v. State, No. 09-13-00409-CR, 2015 WL 3898001, at *9-11 (Tex. App.—Beaumont June 24, 2015) (mem. op., not designated for publication).

^{68.} Dering v. State, 465 S.W.3d 668, 670-72 (Tex. App.-Eastland 2015, no pet.).

^{69.} *R.Z. v. Tex. Dep't of Family & Protective Servs.*, No. 03-14-00412-CV, 2014 WL 5653272, at *3 (Tex. App.—Austin Oct. 29, 2014, no pet.) (mem. op.).

State v. Burns

The victim's mother set up her daughter's Facebook account so that she would receive e-mail alerts every time her daughter received information over Facebook. The victim's mother received an e-mail that her daughter had received a message from the defendant's Facebook account asking for pictures of her daughter. The victim's mother looked at her daughter's computer and found more messages between the victim and the defendant. The victim's mother contacted the police, who seized her daughter's computer as well as the defendant's computer. At trial, the State offered the Facebook messages into evidence, along with e-mails between the defendant and the victim. The court held that more than enough circumstantial evidence existed to authenticate the evidence. In addition to the fact that the defendant admitted that the Facebook account used to send the messages belonged to him, the police were able to independently verify that the Facebook account belonged to the defendant by comparing the profile picture and associated Hotmail e-mail address. Also, transcripts of the same messages were found on both the defendant's and the victim's computers. Finally, the e-mail address linked to the Facebook page was also linked to the defendant's resume and cell phone, and the same pictures were found on both the defendant's cell phone and the victim's computer.⁷⁰

§ 18.2:13 Authenticating Chat Room Content

The *Lorraine* court again offers invaluable insight into authenticating chat room content:

Many of the same foundational issues found encountered when authenticating website evidence apply with equal force to text messages and internet chat room content; however, the fact that chat room messages are posted by third parties, often using "screen names" means that it cannot be assumed that the content found in chat rooms was posted with the knowledge or authority of the website host.⁷¹

One commentator has suggested that the following foundational requirements must be met to authenticate chat room evidence:

^{70.} *State v. Burns*, No. M2014-00357-CCA-R3-CD, 2015 WL 2105543, at *10–12 (Tenn. Crim. App. May 5, 2015).

^{71.} Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 556 (D. Md. 2007).

- (1) evidence that the individual used the screen name in question when participating in chat room conversations (either generally or at the site in question);
- (2) evidence that, when a meeting with the person using the screen name was arranged, the individual showed up;
- (3) evidence that the person using the screen name identified himself as the person in the chat room conversation;
- (4) evidence that the individual had in his possession information given to the person using the screen name; or
- (5) evidence from the hard drive of the individual's computer showing use of the same screen name.⁷²

§ 18.2:14 Relevant Case Law Regarding Authenticating Chat Room Content

In re F.P.

The defendant argued that the testimony of the internet service provider was required, or that of a forensic expert. The court held that circumstantial evidence, such as the use of the defendant's screen name in the text message, the use of the defendant's first name, and the subject matter of the messages all could authenticate the transcripts.⁷³

United States v. Simpson

In *United States v. Simpson*,⁷⁴ the court held that there was ample circumstantial evidence to authenticate printouts of the content of chat room discussions between the defendant and an undercover detective, including use of the e-mail name of the defendant, the presence of the defendant's correct address in the messages, and notes seized at the defendant's home containing the address, e-mail address, and telephone number given by the undercover officer.

^{72.} Lorraine, 241 F.R.D. at 556. (quoting 1 Saltzburg, Federal Rules of Evidence Manual, § 901.02[12]).

^{73.} In re F.P., 878 A.2d 91, 93-94 (2005).

^{74.} United States v. Simpson, 152 F.3d 1241, 1249 (10th Cir. 1998).

§ 18.2

United States v. Tank

Likewise, in *United States v. Tank*,⁷⁵ the court found sufficient circumstantial facts to authenticate chat room conversations, despite the fact that certain portions of the text of the messages in which the defendant had participated had been deleted. The court found the testimony regarding the limited nature of the deletions by the member of the chat room club who had made the deletions and circumstantial evidence connecting the defendant to the chat room, including the use of the defendant's screen name in the messages, were sufficient to authenticate the messages.

United States v. Barlow

On appeal, the defendant asserted that the government had failed to lay the proper foundation for a log from a Yahoo chat room. The appellate court held that the testimony of a witness who had been involved in the chats was sufficient to authenticate the chat log.⁷⁶

§ 18.2:15 Authenticating Stored Data and Records

The Lorraine court observed the following for stored data:

In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. If a computer processes data rather than merely storing it, authentication issues may arise. The need for authentication and an explanation of the computer's processing will depend on the complexity and novelty of the computer processing. There are many stages in the development of computer data where error can be introduced, which can adversely affect the accuracy and reliability of the output. Inaccurate results occur most often because of bad or incomplete data inputting, but can also happen when defective software programs are used or stored-data media become corrupted or damaged.⁷⁷

Further, as authentication issues can arise depending on whether data is stored or processed, it is vital for the practitioner to understand the discovery process involved

^{75.} United States v. Tank, 200 F.3d 627, 629-31 (9th Cir. 2000).

^{76.} United States v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009).

^{77.} Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 543 (D. Md. 2007) (quoting 5 McLaughlin, Weinstein, & Berger, Weinstein's Federal Evidence § 900.06[3] (2d ed. 1998)).

with obtaining ESI, namely how data is processed, how to collect it, and depending on its form, how to properly authenticate it.

"Given the widespread use of computers, there is an almost limitless variety of records that are stored in or generated by computers."⁷⁸ One commentator has observed—

[m]any kinds of computer records and computer-generated information are introduced as real evidence or used as litigation aids at trials. They range from computer printouts of stored digital data to complex computer-generated models performing complicated computations. Each may raise different admissibility issues concerning authentication and other foundational requirements.⁷⁹

The simplest admissibility issues are associated with electronically stored records. "In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues."⁸⁰ Although computer records are the easiest to authenticate, some courts have recognized that more care is required to authenticate these electronic records than traditional "hard copy" records, as demonstrated below.

§ 18.2:16 Relevant Case Law Regarding Authenticating Stored Data and Records

United States v. Meienberg

In *United States v. Meienberg*,⁸¹ the defendant challenged on appeal the admission into evidence of printouts of computerized records of the Colorado Bureau of Investigation, arguing that they had not been authenticated because the government had failed to introduce any evidence to demonstrate the accuracy of the records. The Tenth Circuit disagreed, stating: "Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility."

- 80. Lorraine, 241 F.R.D at 557 (quoting Weinstein's Federal Evidence § 900.06[3]).
- 81. United States v. Meienberg, 263 F.3d 1177, 1180-81 (10th Cir. 2001).

^{78.} Lorraine, 241 F.R.D at 556.

^{79.} Lorraine, 241 F.R.D at 556-57 (quoting Weinstein's Federal Evidence § 900.06[3]).

United States v. Kassimu

To authenticate computer records as business records did not require the maker nor a custodian of the record. Only a witness qualified to explain the recordkeeping system of the organization was required to confirm that the requirements of Federal Rule of Evidence 803(6) had been met, and the inability of a witness to attest to the accuracy of the information entered into the computer did not preclude admissibility.⁸²

Sea-Land v. Lozen

The trial court properly considered electronically generated bill of lading as an exhibit to a summary judgment motion. The only foundation that was required was that the record was produced from the same electronic information that was generated contemporaneously when the parties entered into their contact. The court did not require evidence that the records were reliable or accurate.⁸³

In re Vee Vinhnee

In the case of *In re Vee Vinhnee*,⁸⁴ the bankruptcy appellate panel upheld the trial ruling of a bankruptcy judge excluding electronic business records of the credit card issuer of a Chapter 7 debtor, for failing to authenticate them. The court noted that "it is becoming recognized that early versions of computer foundations were too cursory, even though the basic elements covered the ground." *In re Vee Vinhee*, 336 B.R. at 445–46. The court further observed:

The primary authenticity issue in the context of business records is on what has, or may have, happened to the record in the interval between when it was placed in the files and the time of trial. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created. Hence, the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created.

^{82.} United States v. Kassimu, 188 F. App'x 264 (5th Cir. 2006).

^{83.} Sea-Land Serv., Inc. v. Lozen Int'l, 285 F.3d 808 (9th Cir. 2002).

^{84.} In re Vee Vinhnee, 336 B.R. 437, 445 (B.A.P. 9th Cir. 2005).

In re Vee Vinhee, 336 B.R. at 444. The court reasoned that for paperless electronic records:

The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation.

In re Vee Vinhee, 336 B.R. at 445. In order to meet the heightened demands for authenticating electronic business records, the court adopted, with some modification, an eleven-step foundation proposed by Professor Edward Imwinkelried, viewing electronic records as a form of scientific evidence:

- 1. The business uses a computer.
- 2. The computer is reliable.
- 3. The business has developed a procedure for inserting data into the computer.
- 4. The procedure has built-in safeguards to ensure accuracy and identify errors.
- 5. The business keeps the computer in a good state of repair.
- 6. The witness had the computer readout certain data.
- 7. The witness used the proper procedures to obtain the readout.
- 8. The computer was in working order at the time the witness obtained the readout.
- 9. The witness recognizes the exhibit as the readout.
- 10. The witness explains how he or she recognizes the readout.
- 11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.⁸⁵

^{85.} In re Vee Vinhee, 336 B.R. at 446.

State v. Dunn

Admissibility of computer-generated records "should be determined on the basis of the reliability and accuracy of the process involved."⁸⁶

State v. Hall

"[T]he admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy."⁸⁷

Haas v. State

At trial, the State introduced computer-generated documents from prior DWI convictions to enhance the current conviction. The court of appeals held that the certified document number on each page of each document, coupled with the seal contained on the last page of each document satisfied the authentication rules. It further noted that original seals are not required for public records.⁸⁸

The cases above show that there is a wide disparity between the most lenient positions courts have taken in accepting electronic records as authentic and the most demanding requirements that have been imposed. Further, it would not be surprising to find that, to date, more courts have tended towards the lenient rather than the demanding approach. However, it also is plain that commentators and courts increasingly recognize the special characteristics of electronically stored records, and there appears to be a growing awareness, as expressed in the Manual for Complex Litigation, that courts "should consider the accuracy and reliability of computerized evidence" in ruling on its admissibility. Lawyers can expect to encounter judges in both camps, and in the absence of controlling precedent in the court where an action is pending setting forth the foundational requirements for computer records, there is uncertainty about which approach will be required. Further, although "it may be better to be lucky than good," as the saying goes, counsel would be wise not to test their luck unnecessarily. If it is critical to the success of your case to admit into evidence computer-stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied. If less is required, then luck was with you.

§ 18.2

^{86.} State v. Dunn, 7 S.W.3d 427, 432 (Mo. Ct. App. 1999).

^{87.} State v. Hall, 976 S.W.2d 121, 147 (Tenn. 1998).

^{88.} Haas v. State, 494 S.W.3d 819 (Tex. App.-Houston [14th Dist.] 2016, no pet.).

§ 18.2:17 Authenticating Digital Photographs and Videos

Photographs have been authenticated for decades under rule 901(b)(1) by the testimony of a witness familiar with the scene depicted in the photograph who testifies that the photograph fairly and accurately depicts the scene.⁸⁹ Calling the photographer or offering expert testimony about how a camera works almost never has been required for traditional film photographs. Today, however, most photographs taken and offered as exhibits at trial are digital photographs, which are not made from film, but rather from images captured by a digital camera and loaded into a computer. Digital photographs present unique authentication problems because they are a form of electronically produced evidence that may be manipulated and altered, although traditional authentication rules still apply because film photographs can be manipulated and altered as well, just not as easily. Whether from an original film photograph uploaded into a computer or a digital camera image, digital image enhancement consists of removing, inserting, or highlighting an aspect of the photograph that the technician wants to change.

Some examples illustrated in the Lorraine case are as follows:

Suppose that in a civil case, a shadow on a 35-mm photograph obscures the name of the manufacturer of an offending product. The plaintiff might offer an enhanced image, magically stripping the shadow to reveal the defendant's name. Or suppose that a critical issue is the visibility of a highway hazard. A civil defendant might offer an enhanced image of the stretch of highway to persuade the jury that the plaintiff should have perceived the danger ahead before reaching it In many criminal trials, the prosecutor offers an "improved," digitally enhanced image of fingerprints discovered at the crime scene. The digital image reveals incriminating points of similarity that the jury otherwise would never would have seen.⁹⁰

There are three distinct types of digital photographs that should be considered with respect to authentication analysis: original digital images, digitally converted images, and digitally enhanced images, detailed below.

^{89.} Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 561 (D. Md. 2007).

^{90.} Lorraine, 241 F.R.D. at 561. (quoting Edward J. Imwinkelried, Can this Photo be Trusted?, Trial (Oct. 2005), at 49).

§ 18.2:18 Original Digital Images

An original digital image may be authenticated the same way as a film photograph, that is, by a witness with personal knowledge of the scene depicted who can testify that the photo fairly and accurately depicts it.⁹¹ If a question is raised about the reliability of digital photography in general, the court likely could take judicial notice of it under rule 201.⁹²

Further, even if no witness can testify from personal knowledge that the photo or video accurately depicts the scene, the "silent witness" analysis allows a photo or video to be authenticated by showing a process or system that produces an accurate result.⁹³ Testimony that showed how the storage device was put in the camera, how the camera was activated, the removal of the storage device immediately after the offense, the chain of custody, and how the film was developed/photograph was printed is sufficient to support a trial court's decision to admit evidence.⁹⁴ Photos taken by an ATM were properly authenticated on even less evidence-mere testimony of a bank employee familiar with the operation of the camera and the fact that the time and date were indicated on the evidence were sufficient to authenticate the photos.⁹⁵

§ 18.2:19 Digitally Converted Images

For digitally converted images, that is, film photographs that have been converted into a digital format, authentication requires an explanation of the conversion process. This would require testimony about the conversion process, requiring a witness with personal knowledge that the conversion process produces accurate and reliable images.⁹⁶ "Alternatively, if there is a witness familiar with the scene depicted who can testify that the photo produced from the film when it was digitally converted, no testimony would be needed regarding the process of digital conversion."⁹⁷

97. Lorraine, 241 F.R.D. at 561.

^{91.} Lorraine, 241 F.R.D. at 561.

^{92.} Lorraine, 241 F.R.D. at 561.

^{93.} See Tex. R. Evid. 901(b)(9).

^{94.} Reavis v. State, 84 S.W.3d 716, 719 (Tex. App.-Fort Worth 2002, no pet.).

^{95.} United States v. Fadayini, 28 F.3d 1236, 1241 (D.C. Cir. 1994).

^{96.} Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 561 (D. Md. 2007) (citing rules 901(b)(1), 901(b)(9), and 702).

§ 18.2:20 Digitally Enhanced Images

"For digitally enhanced images it is unlikely that there will be a witness who can testify how the original scene looked if, for example, a shadow was removed, or the colors were intensified."⁹⁸ In such a case, there will need to be proof, permissible under rule 901(b)(9), that the digital enhancement process produces reliable and accurate results, which gets into the realm of scientific or technical evidence under rule 702.⁹⁹ But perhaps because digital-enhancement software is so readily available today, and has become more user-friendly and easy enough for just about anybody to use, expert opinion is not as critical.

Before the current proliferation of such digital-enhancement software, the court in State v. Swinton¹⁰⁰ held that evidence had not been properly authenticated. The defendant was convicted of murder based in part on evidence of computer enhanced images prepared using Adobe Photoshop. The images showed a superimposition of the defendant's teeth over digital photographs of bite marks taken from the victim's body. At trial, the state called the forensic odontologist (bite mark expert) to testify that the defendant was the source of the bite marks on the victim. However, the forensic odontologist testified that he was not familiar with how Adobe Photoshop made the overlay photographs, which involved a multistep process in which a wax mold of the defendant's teeth was digitally photographed and scanned into the computer to then be superimposed on the photo of the victim. The trial court admitted the exhibits over objection, but the state appellate court reversed, finding that the defendant had not been afforded a chance to challenge the scientific or technical process by which the exhibits had been prepared. The court stated that to authenticate the exhibits would require a sponsoring witness who could testify adequately and truthfully as to exactly what the jury was looking at, and the defendant had a right to cross examine the witness concerning the evidence. Because the witness called by the state to authenticate the exhibits lacked the computer expertise to do so, the defendant was deprived of the right to cross examine him.

In reviewing the issue in the Lorraine case, Judge Grimm noted-

Because the process of computer enhancement involves a scientific or technical process, one commentator has suggested the following foundation as a means to authenticate cigitally enhanced photographs under rule

^{98.} Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 561 (D. Md. 2007).

^{99.} Lorraine, 241 F.R.D. at 561.

^{100.} State v. Swinton, 268 Conn. 781, 847 A.2d 921, 950-52 (2004).

901(b)(9): (1) The witness is an expert in digital photography; (2) the witness testifies as to image enhancement technology, including the creation of the digital image consisting of pixels and the process by which the computer manipulates them; (3) the witness testifies that the processes used are valid; (4) the witness testifies that there has been "adequate research into the specific application of image enhancement technology involved in the case"; (5) the witness testifies that the software used was developed from the research; (6) the witness received a film photograph; (7) the witness digitized the film photograph using the proper procedure, then used the proper procedure to enhance the film photograph in the computer; (8) the witness can identify the trial exhibit as the product of the enhancement process he or she performed. [Imwinkelried, Can this Photo be Trusted?, at 54.] The author recognized that this is an "extensive foundation," and whether it will be adopted by courts in the future remains to be seen. Id. However, it is probable that courts will require authentication of digitally enhanced photographs by adequate testimony that a photograph is the product of a system or process that produces accurate and reliable results. Fed. R. Evid. 901(b)(9).¹⁰¹

§ 18.2:21 Relevant Case Law Regarding Authenticating Digital Photographs and Videos

Thierry v. State

A court found the following testimony sufficient to authenticate a video. A witness, who was not present at the time of the incident, described the store's multiplex recording system and its computer systems; he detailed how he was able to link the encoding on the receipts to the time and date that the account was opened, to the transactions in question, to the cashier, to the terminal, and finally to the video camera that recorded the transactions; and he testified that he had personally copied the relevant recordings from the multiplex to the videotape. He further testified that he had viewed the video on the multiplex system, viewed it on the tape on the day that he made the tape, and then viewed it again on the day prior to his testimony and that it fairly and accurately represented what it purported to show. The witness testified that no alterations or deletions were made to the videotape.¹⁰²

^{101.} Lorraine, 241 F.R.D. at 562 (citing Imwinkelried, Can this Photo be Trusted?, at 54).

^{102.} Thierry v. State, 288 S.W.3d 80 (Tex. App.-Houston [1st Dist.] 2009, pet. ref'd).

Brown v. State

Interestingly, a witness may authenticate a photograph without knowing where it was taken, when it was taken, or by whom it was taken, as long as the witness can testify that the photograph accurately represents what it purports to represent.¹⁰³ This holds true for any photograph, not just digital photographs.

Hines v. State

Even though portions of a video may be choppy or contain breaks in the video content, the video can still be authenticated by a witness testifying that the video depicts exactly what it purports to depict.¹⁰⁴

Ruff v. State

At trial, the State offered copies of recordings from the store owner's security cameras. Because the owner did not know how to make copies of the recordings, his daughter videotaped the videos and provided the copies to law enforcement. The defendant objected on the ground of authentication. The court of appeals held that, although owner did not appear to be a native English speaker, his testimony sufficiently established that the videotaped copy was a fair and accurate depiction of the recordings from his security cameras.¹³⁵

Simpson v. State

At trial, the State introduced the police video of a DWI traffic stop and the transportation of the defendant to the police station. The audio cut after the arrest was made. The arresting police officer explained that the microphone's batteries on his bodycam died and explained why the audio in his vehicle was not working during that time. The court of appeals held that the video was admissible, even though portions of the audio were missing.¹⁰⁶

Fowler v. State

106. Simpson v. State, No. 12-00891-CR, 2014 WL 1338310 (Tex. App.—Houston [1st Dist.] Apr. 3, 2014, no pet.) (mem. op., not designated for publication).

^{103.} Brown v. State, No. 12-11-00027-CR 2011 WL 3915663 (Tex. App.—Tyler Sept. 7, 2011, no pet.) (mem. op., not designated for publication).

^{104.} Hines v. State, 383 S.W.3d 615, 625 (Tex. App.-San Antonio, 2012, pet. denied).

^{105.} *Ruff v. State*, No. 06-14-00029-CR, 2014 WL 2917843 (Tex. App.—Texarkana June 25, 2014, no pet.) (not designated for publication).

A store's surveillance camera recorded the defendant committing a theft. The State offered the video at trial, which the trial court admitted. On appeal, defendant argued that it had not be properly authenticated, and the court of appeals reversed. The Texas Court of Criminal Appeals held that "yes, it is possible" for the proponent of a video to sufficiently prove its authenticity without testimony of someone who either witnessed what the video depicts or is familiar with the functioning of the recording device. The court used the distinctive characteristics test to determine that the trial court was within the zone of reasonable disagreement when admitting the video.¹⁰⁷

§ 18.2:22 Authenticating Voice Mail or Other Audio Recordings

Texas Rule of Evidence 901(b)(5) provides that a voice recording may be identified by opinion based on hearing the voice at any time under circumstances connecting it with the alleged speaker.¹⁰⁸ One Texas court has found that a voice mail was not properly authenticated when a witness testified that she recognized the voice as a party's but did not identify the recording or explain the circumstances in which it was made.¹⁰⁹ However, a recording can be properly authenticated even when the witness cannot identify every voice in the recording, so long as those unknown voices are not pertinent to the case.¹¹⁰

§ 18.2:23 Relevant Case Law Regarding Authenticating Voice Mail and Other Audio Recordings

Goodrich v. State

One case lists three methods that can be used to authenticate a voic email: (1) through the testimony of a witness with knowledge that a matter is what it is claimed to be; (2) by opinion based on hearing the voice at any time under circumstances connecting it with the alleged speaker; or (3) demonstrating the identity of a caller by self-identification coupled with additional circumstances, such as the context and timing of the

^{107.} Fowler v. State, 544 S.W.3d 844 (Tex. Crim. App. 2018).

^{108.} Tex. R. Evid. 901(b)(5).

^{109.} Miller v. State, 208 S.W.3d 554, 566 (Tex. App.-Austin 2006, pet. ref'd).

^{110.} See, e.g., Escalona v. State, No. 05-12-01418-CR, 2014 WL 1022330, at *10 (Tex. App.—Dallas Feb. 20, 2014, pet. ref'd) (mem. op., not designated for publication) (holding that "[i]t was not necessary to identify both voices on the phone call recordings in order for the State to prove that the recordings were what the State claimed them to be.") (citing *Banargent v. State*, 228 S.W.3d 393, 401 (Tex. App.—Houston [14th Dist.] 2007, pet. ref'd), and *Jones v. State*, 80 S.W.3d 686 (Tex. App.—Houston [1st Dist.] 2002, no pet.)); *Rios v. State*, No. 10-08-00408-CR, 2009 WL 3766341 (Tex. App.—Waco Nov. 10, 2009, no pet.) (mem. op., not designated for publication).

call, the contents of the statement, and disclosure of knowledge of facts known peculiarly to the speaker.¹¹¹

\$201,000.00 U.S. Currency v. State

In a forfeiture proceeding, a police officer testified that he had participated in an outof-state investigation involving the original owner of the funds. The officer conducted surveillance against the owner and recorded the conversation. The State introduced a recording between the owner and an informant. The owner objected on the grounds that the sponsoring witness could not authenticate the recording because he was not in the physical presence of the owner and informant when it took place. The court held that, because the sponsoring witness had been involved in an investigation involving the owner, he had knowledge of the owner's voice and that the recording was what the State claimed it was.¹¹²

Diamond v. State

The defendant, who was charged with capital murder, made several phone calls from jail in which he discussed various aspects of the crime. During one conversation, the defendant mentioned that there was "a present" in his car. The police searched his vehicle and found a pistol in the spot the defendant had described as containing the "present." Shell casings found at the scene of the murder matched those from the pistol, linking the defendant to the murder. The phone calls were authenticated through the testimony of the custodian of the phone call recording system, who described how the system worked as well as how inmates used an identification number to make calls, and through the police officer who had interviewed defendant and identified the defendant's voice on the recordings.¹¹³

Escalona v. State

At trial, the defendant objected to the authenticity of a jailhouse telephone call on the grounds that the State's witness could only identify the defendant's voice, not that of the other person on the call. The court of appeals held that to properly authenticate the phone call, the State only had to prove the call was linked to the defendant and only had to identify the defendant's voice.¹¹⁴

^{111.} Goodrich v. State, No. 09-10-00167-CR, 2011 WL 1417026 (Tex. App.—Beaumont Apr. 13, 2011) (mem. op., not designated for publication).

^{112. \$201,100.00} U.S. Currency v. State, No. 09-14-00478-CV, 2015 WL 4312536 (Tex. App.-Beaumont July 16, 2015, pet. denied) (mem. op.).

^{113.} Diamond v. State, 496 S.W.3d 124 (Tex. App.-Houston [14th Dist.] June 7, 2016, pet. ref'd).

Moore v. State

A 911 dispatcher testified regarding the recording of a call between the dispatcher and a third party who had called to report an assault that was in progress. Portions of the recording containing radio traffic between the dispatcher and the responding officers had been removed from the tape; however, the dispatcher still identified the recording as a fair and accurate representation of her conversation with the 911 caller. The court of appeals held that, even though those certain audio portions were missing, and even though the dispatcher had testified that she did not know how the recording equipment worked, the recording nevertheless was properly authenticated as to the conversation between the dispatcher and the 911 caller.¹¹⁵

Knight v. State

The court of appeals considered an issue of authentication of 911 calls, even though the defendant had not preserved that issue for appeal.¹¹⁶ The State had presented the testimony from the custodian of records for the El Paso Police Department's 911 call center. The custodian testified regarding the call center's policies on receiving, storing, and retrieving of records. The custodian also testified that she personally retrieved the exhibits for trial and that she knew the retrieved records related to the specific call in question because the numbers on the records correlated to the police number assigned to the case. Furthermore, she testified that the records had continuously been in the custody of the El Paso Police Department and that she put the contents onto a CD, which had her handwriting on it, that enabled her to identify the recording as the same one received by the call center on the day in question. She had also listened to the recording and could identify the call taker's voice.

Practice Tip: A video is typically authenticated by a witness who can testify either that the scene is accurately depicted, or that the recording was made by a reliable method. However, if your witness merely recognizes the people in the video but cannot testify about the scene or how the video was made, you may try admitting solely the audio portion. Your witness can testify that she recognizes some or all the voices, and the other requirements for authenticating a video would not apply.

^{114.} Escalona v. State, No. 05-12-01418-CR, 2014 WL 1022330 (Tex. App.—Dallas Feb. 20, 2014, pet. ref'd) (mem. op., not designated for publication).

^{115.} *Moore v. State*, No. 02-15-00227-CR, 2016 WL 278754 (Tex. App.—Fort Worth Jan. 21, 2016, no pet.) (mem. op., not designated for publication).

^{116.} Knight v. State, No. 08-16-00123-CR, 2018 WL 3867570 (Tex. App.—El Paso Aug. 15, 2018, no pet.) (not designated for publication).
§18.2:24 Conclusion

Judge Grimm gave wise counsel to any lawyer wanting to authenticate evidence:

To prepare properly to address authentication issues associated with electronically generated or stored evidence, a lawyer must identify each category of electronic evidence to be introduced. Then, he or she should determine what courts have required to authenticate this type of evidence, and carefully evaluate the methods of authentication identified in rules 901 and 902, as well as consider requesting a stipulation from opposing counsel, or filing a request for admission of the genuineness of the evidence With this analysis in mind, the lawyer then can plan which method or methods of authentication will be most effective, and prepare the necessary formulation, whether through testimony, affidavit, admission or stipulation. The proffering attorney needs to be specific in presenting the authenticating facts and, if authenticity is challenged, should cite authority to support the method selected.¹¹⁷

An attorney could also ask authenticating questions about ESI during a deposition. An attorney could have the deponent log into various sites during the deposition and testify to the contents. In theory, this would be no different than having a deponent produce a diary and go through it.

§ 18.3 Additional Issues Affecting the Admissibility of ESI

§ 18.3:1 Best-Evidence Rule

Rule 1002 of the Texas Rules of Evidence states that to prove the content of a writing, recording, or photograph, the *origina!* writing, recording, or photograph is required except as otherwise provided.¹¹⁸ Under rule 1001(d), if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original.¹¹⁹

119. Tex. R. Evid. 1001(d).

^{117.} Lorraine, 241 F.R.D. at 562.

^{118.} Tex. R. Evid. 1002 (emphasis added).

to the results of a computer search without qualifying as an expert or presenting computer printouts. In this case, the witness said that a computer search on the bank's computer confirmed that an account number on a suspicious check was fictitious. According to the court, the best-evidence rule was not implicated because the witness was merely explaining the process he went through to determine whether an account number was a valid one with his bank. The court also said that the best evidence was offered to show the nonexistence of a bank account.

In *Milton v. State*, the State transferred a recording to a CD and offered the duplicate into evidence instead.¹²¹ The defendant objected, citing the best-evidence rule. The court stated that a duplicate is admissible to the same extent as an original unless a question is raised as to the authenticity of the original. Stated another way, a duplicate is inadmissible if reasonable jurors might differ as to whether the original is what it is claimed to be. Because the defendant challenged the authenticity of the duplicate CD rather than the original, and the officer testified the copy was an exact duplicate, the best-evidence objection failed.

An objection under Texas Rule of Evidence 1002 is most often relevant in situations where a litigant is seeking to admit copies of text messages, e-mail streams, or chat conversations that have been cut and pasted into an exhibit. In *United States v. Jackson*,¹²² the court sustained the defendant's objection that a cut-and-paste document reflecting instant message conversations between the defendant and a federal agent were inadmissible under the best-evidence rule. Because the document was neither an original under Federal Rule of Evidence 1001 (or a duplicate under rule 1003), the court held that it was inadmissible because "[i]t is clear the proposed document does not accurately reflect the contents of the original."¹²³ If however, the instant messages were independently authenticated and later pasted into a summary exhibit, this exhibit could be admitted under rule 1006.

One interesting issue concerning ESI and the application of the Texas Rules of Evidence regarding original writings is the applicability of rule 1004, which permits the admission of "other evidence" of the contents of a writing if the original is lost,

^{120.} No. B14-91-00458-CR, 1992 WL 133831 (Tex. App.—Houston [14th Dist.] June 18, 1992) (not designated for publication).

^{121.} *Milton v. State*, No. 14-10-00696-CR, 2011 WL 4361482 (Tex. App.—Houston [14th Dist.] Sept. 20, 2011) (mem. op., not designated for publication).

^{122.} United States v. Jackson, 488 F. Supp. 2d 866 (D. Neb. 2007).

^{123.} Jackson, 488 F. Supp. 2d at 871.

Authentication and Admissibility

destroyed, not in Texas, or otherwise unobtainable.¹²⁴ Given how fleeting information posted on the Internet can be, it is likely that there may be occasions where a party must resort to secondary evidence to establish the content of ESI that is lost, destroyed, not in Texas, or otherwise unobtainable.

§ 18.3:2 Hearsay Issues

Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.¹²⁵ The "matter asserted" includes any matter explicitly asserted and any matter implied by a statement, if the probative value of the statement as offered flows from the declarant's belief as to the matter.¹²⁶ Hearsay is inadmissible unless otherwise permitted by the rules or by statute.¹²⁷

Put more simply, any out-of-court statement, except a statement listed in rule 801(e), whether by the witness or another person, is hearsay and is inadmissible to support the truth of a claim, unless permitted by another rule. However, otherwise inadmissible hearsay admitted without objection should not be denied probative value merely because it is hearsay.¹²⁸ If it can be shown that a statement is nonhearsay or that it falls within a hearsay exception, the statement can be admissible as probative evidence.¹²⁹

"The twenty-four hearsay exceptions listed in Texas Rule [of Evidence] 803 may be roughly categorized into (1) unreflective statements, (2) reliable documents, and (3) reputation evidence. The rationale for all of the exceptions is that, over time, experience has shown that these types of statements are generally reliable and trust-worthy."¹³⁰ However, all hearsay exceptions require a showing of trustworthiness.¹³¹

- 127. Tex. R. Evid. 802; see, e.g., Tex. R. Evid. 107, 801(e), 803, 804.
- 128. Tex. R. Evid. 802.
- 129. See Miranda v. State, 813 S.W.2d 724, 735 (Tex. App.-San Antonio 1991, pet ref'd).
- 130. Fischer v. State, 252 S.W.3d 375, 379 (Tex. Crim. App. 2008).
- 131. Robinson v. Harkins & Co., 711 S.W.2d 619, 621 (Tex. 1986).

^{124.} Tex. R. Evid. 1004.

^{125.} Tex. R. Evid. 801(d).

^{126.} Tex. R. Evid. 801(c).

§ 18.3:3 Unreflective Statements

Evidence obtained from e-mail, text messaging, or social networking sites such as Facebook, MySpace, or Twitter is often relevant in many types of cases. The evidence may be nonhearsay to the extent that it is an admission by a party-opponent, but there may be times where statements by others are relevant. Of the hearsay exceptions, Texas Rule of Evidence 803(1)–(3) can be especially useful in admitting these types of statements. Those are the exceptions for present sense impression, excited utterance, and then-existing condition. Electronic communication is particularly prone to candid statements of the declarant's state of mind, feelings, emotions, and motives.¹³² Further, such messages are often sent while events are unfolding. The logic of the existing exceptions can be applied to admit even new forms of communication.

Present Sense Impression: A statement describing or explaining an event or condition, made while or immediately after the declarant perceived it.¹³³

Unlike the excited-utterance exception, the rationale for this exception stems from the statement's contemporaneity, not its spontaneity.¹³⁴ The present-sense-impression exception to the hearsay rule is based on the premise that the contemporaneity of the event and the declaration ensures reliability of the statement. The rationale underlying the present sense impression is that (1) the statement is safe from any error of the defect of memory of the declarant because of its contemporaneous nature, (2) there is little or no time for a calculated misstatement, and (3) the statement will usually be made to another (the witness who reports it) who would have an equal opportunity to observe and therefore check a misstatement.¹³⁵ The *Fischer* case states the following:

The rule is predicated on the notion that the utterance is a reflex product of immediate sensual impressions, unaided by retrospective mental processes. It is instinctive, rather than deliberate. If the declarant has had time to reflect upon the event and the conditions he observed, this lack of contemporaneity diminishes the reliability of the statements and renders them inadmissible under the rule.

Once reflective narratives, calculated statements, deliberate opinions, conclusions, or conscious thinking-it-through statements enter the picture, the

^{132.} Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 570 (D. Md. 2007).

^{133.} Tex. R. Evid. 803(1) (emphasis added).

^{134.} Rabbani v. State, 847 S.W.2d 555, 560 (Tex. Crim. App. 1992).

^{135.} Rabbani, 847 S.W.2d at 560.

Authentication and Admissibility

present sense impression exception no longer allows their admission. Thinking about it destroys the unreflective nature required of a present sense impression.¹³⁶

Excited Utterance: A statement relating to a startling event or condition, made while the declarant was under the stress or excitement that it caused.¹³⁷

The excited-utterance exception is broader than the present-sense-impression exception.¹³⁸ While a present-sense-impression statement must be made while the declarant was perceiving the event or condition, or immediately thereafter, under the excitedutterance exception, the startling event may trigger a spontaneous statement that relates to a much earlier incident.¹³⁹ No independent evidence of that earlier incident need exist; the trial court decides whether sufficient evidence of the event exists, and may consider the excited utterance itself to make that determination.¹⁴⁰ The *Goodman* case states the following:

For the excited-utterance exception to apply, three conditions must be met: (1) the statement must be a product of a startling occurrence that produces a state of nervous excitement in the declarant and renders the utterance spontaneous and unreflecting, (2) the state of excitement must still so dominate the declarant's mind that there is no time or opportunity to contrive or misrepresent, and (3) the statement must relate to the circumstances of the occurrence preceding it. The critical factor in determining when a statement is an excited utterance under rule 803(2) is whether the declarant was still dominated by the emotions, excitement, fear, or pain of the event. The time elapsed between the occurrence of the event and the utterance is only one factor considered in determining the admissibility of the hearsay statement. That the declaration was a response to questions is likewise only one factor to be considered and does not alone render the statement inadmissible.¹⁴¹

^{136.} Fischer v. State, 252 S.W.3d 375, 381 (Tex. Crim. App. 2008) (internal quotations and citations omitted).

^{137.} Tex. R. Evid. 803(2).

^{138.} McCarty v. State, 257 S.W.3d 238, 240 (Tex. Crim. App. 2008).

^{139.} McCarty, 257 S.W.3d at 240.

^{140.} Coble v. State, 330 S.W.3d 253, 294-95 (Tex. Crim. App. 2010).

^{141.} Goodman v. State, 302 S.W.3d 462, 472 (Tex. App.—Texarkana 2009, pet. ref'd) (internal quotations and citations omitted).

Then-Existing Mental, Emotional, or Physical Condition: A statement of the declarant's then existing state of mind, emotion, sensation, or physical condition (such as motive, intent, or plan) or emotional, sensory, or physical condition (such as mental feeling, pain, or bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the validity or terms of the declarant's will.¹⁴²

Texas courts have held that the type of statement contemplated by this rule includes a statement that on its face expresses or exemplifies the declarant's state of mind—such as fear, hate, love, and pain.¹⁴³ For example, a person's statement regarding her emotional response to a particular person qualifies as a statement of then-existing state of emotion under rule 803(3).¹⁴⁴ However, a statement is inadmissible if it is a statement of memory or belief offered to prove the fact remembered or believed.¹⁴⁵ One court offers the following explanation of rule 803(3)'s "exception to the exception":

Case law makes it clear that a witness may testify to a declarant saying "I am scared," but not "I am scared because the defendant threatened me." The first statement indicates an actual state of mind or condition, while the second statement expresses belief about why the declarant is frightened. The phrase "because the defendant threatened me" is expressly outside the state-of-mind exception because the explanation for the fear expresses a belief different from the state of mind of being afraid.¹⁴⁶

§ 18.3:4 Reliable Documents

The second category of hearsay exceptions, reliable documents, can also include a variety of computer- or Internet-stored data. Anything from online flight schedules to personal financial records to e-mails could potentially be admitted under these existing hearsay exceptions.

Recorded Recollection: A record that is on a matter the witness once knew about but now cannot recall well enough to testify fully and accurately; was made or adopted by the witness when the matter was fresh in the witness's memory; and accu-

145. Tex. R. Evid. 803(3).

146. Delapaz v. State, 228 S.W.3d 183, 207 (Tex. App.—Dallas 2007, pet. ref'd) (quoting United States v. Ledford, 443 F.3d 702, 709 (10th Cir. 2005)).

^{142.} Tex. R. Evid. 803(3).

^{143.} Garcia v. State, 246 S.W.3d 121, 132 (Tex. App.-San Antonio 2007, pet. ref'd).

^{144.} Garcia, 246 S.W.3d at 132.

rately reflects the witness's knowledge, unless the circumstances of the record cast doubt on its trustworthiness. If admitted, the record may be read into evidence but may be received as an exhibit only if offered by an adverse party.¹⁴⁷

For a statement to be admissible under rule 803(5)-

(1) the witness must have had firsthand knowledge of the event, (2) the statement must be an original memcrandum made at or near the time of the event while the witness had a clear and accurate memory of it, (3) the witness must lack a present recollection of the event, and (4) the witness must vouch for the accuracy of the written memorandum.¹⁴⁸

To meet the fourth element-

the witness may testify that she presently remembers recording the fact correctly or remembers recognizing the writing as accurate when she read it at an earlier time. But if her present memory is less effective, it is sufficient if the witness testifies that she knows the memorandum is correct because of a habit or practice to record matters accurately or to check them for accuracy. At the extreme, it is even sufficient if the individual testifies to recognizing her signature on the statement and believes the statement is correct because she would not have signed it if she had not believed it true at the time.¹⁴⁹

Records of Regularly Conducted Activity: A record of an act, event, condition, opinion, or diagnosis if the record was made at or near the time by—or from information transmitted by—someone with knowledge; the record was kept in the course of a regularly conducted business activity; making the record was a regular practice of that activity; all these conditions are shown by the testimony of the custodian or another qualified witness, or by affidavit or unsworn declaration that complies with rule 902(10); and the opponent fails to demonstrate that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness. "Business" as used in this paragraph includes every kind of regular organized activity whether conducted for profit or not.¹⁵⁰

^{147.} Tex. R. Evid. 803(5).

^{148.} Johnson v. State, 967 S.W.2d 410, 416 (Tex. Crim. App. 1998).

^{149.} Johnson v. State, 967 S.W.2d at 416.

^{150.} Tex. R. Evid. 803(6).

ity, the records can be admitted under this exception with the spouse as the sponsoring witness, without a business records affidavit. Courts have admitted check registers, medical bills and receipts, and canceled checks in this way.¹⁵¹

The predicate for admissibility under the business records exception is established if the party offering the evidence establishes that the records were generated pursuant to a course of regularly conducted business activity and that the records were created by or from information transmitted by a person with knowledge, at or near the time of the event.¹⁵²

Business records that have been created by one entity but which have become another entity's primary record of the underlying transaction may be admissible pursuant to rule 803(6).¹⁵³

Although rule 803(6) does not require the predicate witness to be the record's creator or have personal knowledge of the content of the record, the witness must have personal knowledge of the manner in which the records were prepared.¹⁵⁴

In order for a compilation of records to be admitted, there must be a showing that the authenticating witness or another person compiling the records had personal knowledge of the accuracy of the statements in the documents.¹⁵⁵ However, documents written in preparation of litigation indicate a lack of trustworthiness and do not qualify as business records under the above rule.¹⁵⁶

Market Reports, Commercial Publications: Market quotations, lists, directories, or other compilations that are generally relied on by the public or by persons in particular occupations.¹⁵⁷

157. Tex. R. Evid. 803(17).

^{151.} See, e.g., Sabatino v. Curtiss Nat'l Bank, 415 F.2d 632, 634 (5th Cir. 1969); In re M.M.S., 256 S.W.3d 470, 477 (Tex. App.—Dallas 2008, no pet.); Strahan v. Strahan, No. 01-01-00614-CV, 2003 WL 22723432, at *8 (Tex. App.—Houston [1st Dist.] Nov. 20, 2003, no pet.) (mem. op.).

^{152.} Martinez v. Midland Credit Management, Inc., 250 S.W.3d 481, 485 (Tex. App.-El Paso 2008, no pet).

^{153.} Nat'l Health Res. Corp. v. TBF Fin., LLC, 429 S.W.3d 125, 130 (Tex. App.-Dallas 2014, no pet.).

^{154.} Barnhart v. Morales, 459 S.W.3d 733, 744 (Tex. App.-Houston [14th Dist.] 2015, no pet.).

^{155.} In re E.A.K., 192 S.W.3d 133, 143 (Tex. App.-Houston [14th Dist.] 2006, pet. denied).

^{156.} Campos v. State, 317 S.W.3d 768, 778 (Tex. App.-Houston [1st Dist.] 2010, pet. ref'd).

Authentication and Admissibility

"Where it is proven that publications of market prices or statistical compilations are generally recognized as reliable and regularly used in a trade or specialized activity by persons so engaged, such publications are admissible for the truth of the matter published."¹⁵⁸ This exception also applies to drug labels if there is sufficient reliability that the drugs had not been changed since the date of packaging.¹⁵⁹ A variety of potentially relevant commercial data published online can be admissible under this exception.

§ 18.3:5 Statements That Are Not Hearsay

Evidence constitutes hearsay only if it is (1) an assertive statement (2) by an out-ofcourt declarant (3) offered to prove the truth of the assertion.¹⁶⁰

Computer Generated "Statements": "Cases involving electronic evidence often raise the issue of whether electronic writings constitute 'statements' under rule 801(a). Where the writings are non-assertive, or not made by a 'person,' courts have held that they do not constitute hearsay, as they are not 'statements."¹⁶¹ This refers to computer-generated statements made by an internal operation of the computer, such as the date and time that a hotel room card reader reads a card key or the self-generated print out from an intoxilyzer instrument, rather than data that was entered by a person and subsequently printed out.¹⁵² Even though these statements may be computer-generated, evidence must still support that the computer process is accurate and reliable.¹⁶³

Metadata: Metadata is the computer-generated data about a file, including date, time, past saves, edit information, etc. It would likely be considered a nonstatement under the above logic, and therefore nonhearsay. It remains important to properly satisfy authentication requirements. A higher authentication standard may apply because it is computer-processed data, rather than merely computer-stored data.

163. See Miller v. State, 208 S.W.3d 554, 552–64 (Tex. App.—Austin 2006, pet. ref'd) (holding that, because no evidence was admitted that self-gererated phone bill or process to create such bill was accurate, trial court erred by admitting phone bill over hearsay objection).

^{158.} Patel v. Kuciemba, 82 S.W.3d 589, 594 (Tex. App.—Corpus Christi-Edinburg 2002, pet. denied).

^{159.} Shaffer v. State, 184 S.W.3d 353, 362 (Tex. App.-Fort Worth 2006, pet. ref'd).

^{160.} Edward J. Imwinkelreid, Evidentiary Foundations §10.01, p. 407 (7th ed., 2008).

^{161.} Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 564 (D. Md. 2007).

^{162.} See, e.g., Stevenson v. State, 920 S.W.2d 342, 343–44 (Tex. App.—Dallas 1996, no pet.) (intoxilyzer); *Murray v. State*, 804 S.W.2d 279, 283–84 (Tex. App.—Fort Worth 1991, pet. ref'd) (hotel room card reader).

However, because metadata is normally hidden and usually not intended to be reviewed, several states have issued ethics opinions concluding that it is unethical to mine inadvertently produced metadata.¹⁶⁴ A few ethics opinions have held that mining metadata is not unethical.¹⁶⁵ Some states require it to be determined on a case-by-case basis.¹⁶⁶

Texas issued an ethics opinion at the end of 2016 about metadata.¹⁶⁷ While it does not directly address mining for metadata, it does instruct that attorneys have a duty to be competent when dealing with electronic documents and to scrub metadata so that a client's confidential information will not be inadvertently disseminated to opposing counsel.¹⁶⁸ It also states that, while lawyers have no duty to tell the sending lawyer that metadata containing confidential information was received, lawyers must continue to follow other ethical rules by not misleading the court.¹⁶⁹ Thus, if a lawyer makes a proposition to the court that would not be misleading without the knowledge of the confidential information, but would be misleading with the knowledge of the confidential information, whether the lawyer inadvertently saw it or mined for it.

Admissions by a Party-Opponent: The statement is offered against an opposing party and:

- 1. was made by the party in an individual or representative capacity;
- 2. is one the party manifested that it adopted or believed to be true;
- 3. was made by a person whom the party authorized to make a statement on the subject;
- 4. was made by the party's agent or employee on a matter within the scope of that relationship and while it existed; or

169. Tex. Comm. on Prof'l Ethics, Op. 665 (2016).

^{164.} See, e.g., Miss. Bar Ethics Comm., Op. 259 (2012); N.C. State Bar Ethics Comm., 2009 Formal Ethics Op. 1 (2010); Me. Bd. of Overseers, Op. 196 (2008).

^{165.} See, e.g., Or. State Bar Legal Ethics Comm., Op. 2011-187 (2015); Co. Bar Ass'n Ethics Comm., Op. 119 (2008); Am. Bar Ass'n Standing Comm. on Ethics & Prof'l Responsibility, Op. 06-442 (2006).

^{166.} See Minn. Lawyers Prof'l Responsibility Board, Op. 22 (2010); Penn. Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Op. 2009-100 (2009).

^{167.} Tex. Comm. on Prof'l Ethics, Op. 665 (2016).

^{168.} Tex. Comm. on Prof'l Ethics, Op. 665 (2016).

5. was made by the party's co-conspirator during and in furtherance of the conspiracy.¹⁷⁰

The exemption for admissions by a party-opponent is extremely useful in overcoming a hearsay objection to things like texts, e-mails, and Facebook wall posts. Electronic evidence will meet this hearsay exemption if it is properly authenticated to have been written/posted/created by the party against whom it is used.¹⁷¹

§ 18.3:6 Emojis/Emoticons

An "emoticon" is "a combination of typed keyboard characters used . . . to represent a stylized face meant to convey the writer's tone."¹⁷² An "emoji" is "an emoticon or other image in [a standardized] set."¹⁷³ Emoticons and emojis are now mainstream in society and are becoming more prevalent in the law, and cases are beginning to cite to them more often.¹⁷⁴ Cases have not directly held whether emojis or emoticons themselves are statements such that they would fall under the hearsay rules. But under the definition of hearsay, a written verbal expression or nonverbal conduct is a statement.¹⁷⁵ Furthermore, drawings have been held to be admissible under hearsay exceptions.¹⁷⁶ Therefore, there is no reason why emoticons or emojis, computer images used to convey the writer's tone or the actual thing the emoji depicts, should not fall under the hearsay rules. When seeking to admit or object to evidence that contains emoticons or emojis, make your argument specific and include the emoticons or emojis accordingly.

171. See, e.g., Cook v. State, 460 S.W.3d 703, 713 (Tex. App.—Eastland 2015, no pet.) (text messages); Massimo v. State, 144 S.W.3d 210, 215–17 (Tex. App.—Fort Worth 2004) (e-mails).

172. Ukwuachu v. State, No. PD-0366-17, 2018 WL 2711167, at *6, fn.12 (Tex. Crim. App. June 6, 2018), reh'g denied (July 25, 2018) (Yeary, J., concurring) (quoting Garner's Modern English Usage 476 (4th ed. 2014)).

173. Ukwuachu, 2018 WL 2711167, at *6, fn.12.

174. See, e.g., United States v. Schweitzer, No. ACM 39212, 2018 WL 3326645, at *2, *6 (A.F. Ct. Crim. App. May 8, 2018), review denied, 78 M.J. 110 (C.A.A.F. 2018); Ukwuachu, 2018 WL 2711167, at *6.

175. Tex. R. Evid. 801(a).

176. See Mims v. State, No. 03-13-00266-CR, 2015 WL 7166026, at *6 (Tex. App.—Austin Nov. 10, 2015, pet. ref'd) (mem. op., not designated for publication) (drawings by a child of the child frowning or smiling represent the child's then-existing emotion and are admissible under 803(3)).

^{170.} Tex. R. Evid. 801(e)(2).

§ 18.3:7 Relevant Cases Regarding ESI and Hearsay

United States v. Khorozian

"[N]either the header nor the text of the fax was hearsay. As to the header, '[u]nder FRE 801(a), a statement is something uttered by "a person," so nothing "said" by a machine is hearsay."¹⁷⁷

United States v. Safavian

Holding that portions of e-mail communications that make imperative statements instructing defendant what to do or asking questions are nonassertive verbal conduct that does not fit within the definition of hearsay.¹⁷⁸

Telewizja Polska USA, Inc. v. Echostar Satellite Corp.

Finding that images and text posted on website offered to show what the website looked like on a particular day were not "statements" and therefore fell outside the reach of the hearsay rule.¹⁷⁹

Perfect 10, Inc. v. Cybernet Ventures, Inc.

Finding that images and text taken from website of defendant not hearsay "to the extent these images and text are being introduced to show the images and text found on the websites, they are not statements at all—and thus fall outside the ambit of the hearsay rule."¹⁸⁰

United States v. Rollins

Computer generated records are not hearsay: the role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer-generated record in this case. Instead, the admissibility of the computer tracing

§ 18.3

^{177.} United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003).

^{178.} United States v. Safavian, 435 Supp. 2d 36, 44 (D.D.C. 2006).

^{179.} Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02 C 3293, 2004 WL 2367740 (N.D. Ill. Oct. 15, 2004).

^{180.} Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1155 (C.D. Cal. 2002), abrogated on other grounds, eBay, Inc. v. MercExchange, LLC, 547 U.S. 388 (2006).

State v. Dunn

Because records of this type [computer-generated telephone records] are not the counterpart of a statement by a human declarant, which should ideally be tested by crossexamination of that declarant, they should not be treated as hearsay, but rather their admissibility should be determined on the reliability and accuracy of the process involved.¹⁸²

State v. Hall

Reviewing the admissibility of computer-generated records and holding-

[t]he role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy.¹⁸³

Massimo v. State

The *Massimo* case has a description of the authentication of a party's e-mails as well as a discussion of whether the e-mails meet the hearsay exemption for admission by party opponent or the hearsay exception for a statement against interest.¹⁸⁴

In re T.T.

Statements by a party on his MySpace page were non-hearsay as admissions by a party-opponent.¹⁸⁵

Bailey v. State

185. In re T.T., 228 S.W.3d 312, 316-17 (Tex. App.-Houston [14th Dist.] 2007, pet. denied).

^{181.} United States v. Rollins, No. ACM34515, 2004 WL 26780, at *9 (A.F. Ct. Crim. App. Dec. 24, 2003), aff'd in part, rev'd in part and remanded, 61 M.J. 338 (C.A.A.F. 2005).

^{182.} State v. Dunn, 7 S.W.3d 427, 432 (Mo. Ct. App. 1999).

^{183.} State v. Hall, 976 S.W.2d 121, 147 (Tenn. 1998).

^{184.} Massimo v. State, 144 S.W.3d 210, 215-17 (Tex. App.-Ft. Worth 2004).

Affirming admission of the defendant's chat room admissions over hearsay objection.¹⁸⁶

People v. Johnson

At trial, defendant sought to admit evidence reflecting that the victim had "liked" certain sexually suggestive posts. The prosecutor argued that the "likes" were inadmissible hearsay. The court of appeals agreed and held that the "likes" attributed to the victim were hearsay.¹⁸⁷

BP Expl. & Prod. Inc. v. Cashman Equip. Corp.

In a breach of contract suit, the defendants sought to strike the plaintiff's summary judgment evidence, which included images of the defendants' websites. The United States Court for the Southern District of Texas held that images of the defendants' website constituted admissions of a party-opponent and were, therefore, admissible as non-hearsay.¹⁸⁸

Cook v. State

The State used a confidential informant to set up a drug buy with defendant. The informant sent and received text messages with the defendant to set up the details of the drug buy. The State properly authenticated the text messages and offered the text messages into evidence. The defendant objected on the grounds that the text messages were hearsay. The court of appeals held that, because the text messages had been properly authenticated, they were properly admitted as admissions of a party-opponent.¹⁸⁹

Jimenez, v. State

When the defendant was arrested, the police found a cell phone containing several incriminating text messages. Those messages were sent and received within twenty-four hours of the crime. The messages also corroborated the defendant's statements to police about where he was traveling. The court of appeals held that the trial court

^{186.} Bailey v. State, No. 05-08-01590-CR, 2009 WL 4725348, at *6 (Tex. App.—Dallas, Dec. 11, 2009, pet. ref'd) (not designated for publication).

^{187.} People v. Johnson, 28 N.Y.S.3d 783 (N.Y. Co. Ct. 2015).

^{188.} BP Expl. & Prod. Inc. v. Cashman Equip. Corp., No. Civ. A. H-13-3046, 2016 WL 1387907 (S.D. Tex. Apr. 8, 2016).

^{189.} Cook v. State, 460 S.W.3d 703 (Tex. App.-Eastland 2015, no pet.).

could have reasonably found that the text messages, which were offered against the defendant, were made by the defendant and were therefore admissions by a party opponent.¹⁹⁰

Bezerra v. State

The defendant was convicted of four counts of indecency with a child. During the investigation, the complainants were interviewed on videotape. A police officer watched the recorded interviews and testified in reliance upon the recordings. The defendant cross-examined the police officer regarding the interviews, particularly about the complainants' nonverbal communications during the interviews. When the State offered the recordings, the defendant objected that they were hearsay. The State argued that, because defendant had inquired about the interviews, the recordings should be admitted under the rule of optional completeness. The court of appeals held that the trial court did not abuse its discretion by admitting the interviews. The rule of optional completeness allows for the introduction of otherwise inadmissible evidence when that evidence is necessary to fully and fairly explain a matter opened by the adverse party. The defendant's cross-examination regarding the interviews because the recordings could explain the nonverbal conduct better than the police officer.¹⁹¹

In re Courtney

A bankruptcy court excluded computer records offered under the "business records" exception because the circumstances of their preparation indicated a lack of trustworthiness. Neither the forensic accountant nor the president of the employer testified how the computer records were stored, found, or collected "to ensure that they were, in fact, recovered from a secure computer database used by the Debtor at [the place of employment] and to the exclusion of other employees."¹⁹²

United States v. Johnson

The defendant was charged with conspiring to participate in a racketeering enterprise to distribute controlled substances. He had posted a rap video to his Instagram account. The government moved in limine to admit the video as an adoptive statement

^{190.} Jimenez v. State, No. 05-13-01523-CR, 2014 WL 6678073 (Tex. App.—Dallas Nov. 25, 2014, no pet.) (not designated for publication).

^{191.} Bezerra v. State, 485 S.W.3d 133 (Tex. App.-Amarillo 2016, pet. ref'd).

^{192.} In re Courtney, 596 B.R. 645 (Bankr. S.D. Ohio 2019).

of the defendant because he had posted it to his Instagram account with the comment: "Tha video up nicca! they welcomed me home like it was 88 [emojis]. Real luv never fails" The court found that the defendant did not adopt the video in its entirety just because he posted it on his Instagram account.

Every day millions of individuals post the statements of others—in video, audio, and written form—to their own social media accounts. One need not look far to find examples where such actions do not constitute an endorsement of the statement, let alone a full-fledged adoption of the statement sufficient to justify its admission at trial against the individual who posted it Nor is there any indication from the message allegedly posted by [defendant] that he authored or adopted the video as a whole—including its production, effects, and the statements of others.¹⁹³

Ghanam v. Does

A defamatory case involving missing road salt and new garbage trucks for the city. Someone responded to an online forum thread that a public official was responsible for stealing the road salt and purchasing new garbage trucks to make more money from a side business selling tires. The Michigan Court of Appeals interpreted the ":P" (sticking tongue out emoji) included in the posts to mean sarcasm, so the statements connected with that emoji "cannot be taken seriously as asserting a fact," so they were not defamatory.¹⁹⁴

Bland v. Roberts

Employee of incumbent sheriff "liked" the opposing candidate's social media campaign page and was terminated. The Fourth Circuit held that "liking a political candidate's campaign page . . . is the Internet equivalent of displaying a political sign in one's front yard, which the Supreme Court has held is substantive speech."¹⁹⁵ Although this case did not directly address whether "liking" a social media page or post could be hearsay, holding that it is substantive speech certainly opens the door to that argument. And depending on who "liked" something and who is offering the "like," it could be an admission by a party-opponent.

^{193.} United States v. Johnson, 280 F. Supp. 3d 772 (D. Md. 2017).

^{194.} Ghanam v. Does, 303 Mich. App. 522, 549 N.W.2d 128 (2014).

^{195.} Bland v. Roberts, 730 F.3d 368, 386 (4th Cir. 2013).

§ 18.4 Unfair Prejudice

If an attorney trying to keep a piece of evidence out has failed to block the evidence based on relevance, authenticity, hearsay, or the original writing rule, the final step is the requirement to balance the evidence's probative value against the potential for unfair prejudice, or other harm, under Texas Rule of Evidence 403. This rule states: "The court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, or needlessly presenting cumulative evidence."¹⁹⁶

Although rule 403 can be used in combination with any other rule of evidence to assess the admissibility of electronic evidence, courts are particularly likely to consider whether the admission of electronic evidence would be unduly prejudicial in certain circumstances, as shown below.

§ 18.5 Relevant Case Law Regarding ESI and Unfair Prejudice

§ 18.5:1 Offensive Language

When the evidence would contain offensive or highly derogatory language that may provoke an emotional response.

Monotype Corp. PLC v. Int'l Typeface Corp.

Finding that trial court properly excluded an e-mail from a Microsoft employee under rule 403 that contained a "highly derogatory and offensive description of . . . [another company's] director."¹⁹⁷

United States v. Mills

The court held that the probative value of rap lyrics and videos was not substantially outweighed by a danger of unfair prejudice because "rap, as an aspect of the larger cultural movement of hip hop, is a mainstream and widely recognized music genre." Accordingly, the court found "it highly unlikely that any reasonable juror nowadays could conclude that [defendant] is guilty of racketeering conspiracy merely because the rap songs contain potentially offensive themes."¹⁹⁸

^{196.} Tex. R. Evid. 403.

^{197.} Monotype Corp. PLC v. Int'l Typeface Corp., 43 F.3d 443, 450 (9th Cir. 1994).

§ 18.5:2 Computer Animations

When analyzing computer animations, to determine if there is a substantial risk that the jury may mistake them for the actual events in the litigation.

Friend v. Time Mfg. Co.

The question is simply whether the animation accurately demonstrates the scene of the accident, and whether the probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.¹⁹⁹

State v. Sayles

The appellate court found no error in the trial court's admission of computer animation slides showing effects of shaken infant syndrome, finding that the trial court properly considered the state version of rule 403 and admitted evidence with a cautionary instruction that the evidence was only an illustration, not a re-creation of the actual crime.²⁰⁰

Pugh v. State

In a murder trial where the defendant ran over the victim with his pickup, the trial court excluded one animation reconstructing the crime but admitted three others. The animation that was excluded was a first-person view from the point of the defendant driving the vehicle. The three that were admitted were from a distance and showed "nothing gruesome." When shown to the jury, the trial court instructed them "that the 'animation is a visualization of the expert's opinion' and 'may be considered by the jury only to the extent that the jury believes beyond a reasonable doubt that other evidence introduced by the State supports the events as depicted in the animation." The court held that the trial court did not err because the animation was based on objective data and did not attempt to portray the victim's actions prior to being run over by the defendant's pickup.²⁰¹

^{198.} United States v. Mills, 367 F. Supp. 3d 664, 672 (E.D. Mich. 2019).

^{199.} Friend v. Time Manufacturing Co., No. 03-343-TUC-CKJ, 2006 WL 2135807, at * 7 (D. Ariz. July 28, 2006).

^{200.} State v. Sayles, 662 N.W. 2d 1, 11 (Iowa 2003).

^{201.} Pugh v. State, No. 11-17-00216-CR, 2019 WL 4130793, at *2 (Tex. App.—Eastland Aug. 30, 2019, pet. filed Oct. 31, 2019) (mem. op., not designated for publication).

§ 18.6

§ 18.5:3 Summaries

When considering the admissibility of summaries of voluminous electronic writings, recordings or photographs under rule 1006.

"Summary evidence is subject to the balancing test under rule 403 that weighs the probative value of evidence against its prejudicial effect."²⁰²

§ 18.5:4 Reliability and Accuracy

In circumstances when the court is concerned as to the reliability or accuracy of the information that is contained within the electronic evidence.

St. Claire v. Johnny's Oyster & Shrimp Inc.

The court expressed extreme skepticism regarding the reliability and accuracy of information posted on the Internet, referring to it variously as "voodoo information." Although the court did not specifically refer to rule 403, the possibility of unfair prejudice associated with the admissibility of unreliable or inaccurate information, as well as for confusion of the jury, makes rule 403 a likely candidate for exclusion of such evidence.²⁰³

§ 18.6 Conclusion

Chief United States Magistrate Judge Paul W. Grimm's 2007 memorandum opinion in *Lorraine v. Markel American Ins. Co.*²⁰⁴ remains today as one of the most comprehensive dissertations of the issues surrounding the admissibility of ESI. At the conclusion of what is essentially a 101-page treatise on evidentiary issues relating to ESI, Judge Grimm explains:

The discussion above highlights the fact that there are five distinct but interrelated evidentiary issues that govern whether electronic evidence will be admitted into evidence at trial or accepted as an exhibit in summary judgment practice. Although each of these rules may not apply to every exhibit offered, as was the case here, each still must be considered in evaluating how to secure the admissibility of electronic evidence to support

^{202.} Weinstein's Federal Evidence § 1006.38[3].

^{203.} St. Claire v. Johnny's Oyster & Shrimp Inc., 76 F. Supp. 2d 773 (S.D. Tex. 1999).

^{204.} Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007).

will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try. The Court hopes that the explanation provided in this memorandum order will assist in that endeavor.²⁰⁵

In echoing the sentiments of Judge Grimm, it is hoped that the information provided in this chapter will also assist the reader in his or her efforts to secure the admissibility of ESI and "get it right on the first try."

205. Lorraine, 241 F.R.D. at 585.

Chapter 19

Ethical Issues in E-Discovery

Kathy Owen Brown¹

§ 19.1 Introduction

When the Texas Disciplinary Rules of Professional Conduct and American Bar Association (ABA) Model Rules of Professional Conduct were promulgated, electronically stored information ("ESI"), electronic discovery ("e-discovery"), and everything that came along with the "technology age" were likely not contemplated by the drafters. However, even though these things may not have been contemplated, these disciplinary rules contain rules that can be land mines for attorneys when venturing into the world of e-discovery and technology if they are not prepared. The rules require cooperation, competence, confidentiality, candor, and diligence. Social networking has also opened up a new set of potential ethical issues for attorneys. Attorneys must keep their ethical obligations in mind when dealing with the technological advances in our modern age.

§ 19.2 Four Cs and a D of Ethical Issues in E-Discovery

§ 19.2:1 Cooperation

In practice today, the costs of litigation associated with e-discovery can often dwarf those associated with the rest of the matter. Parties will sometimes settle a matter they otherwise would not because the discovery costs exceed any potential value of the case. Parties have sometimes decided to forego pursuing a potential claim due to the risk of high discovery costs. If a party has not received a "smoking gun" from the opposition in discovery, the answer could never be that the document never existed, and instead it seeks spoliation sanctions. Defending a spoliation allegation is very costly, even if there are no sanctions awarded.

In our current legal atmosphere, it often seems that cooperation has been lost under an argument for zealously representing clients. The preamble to the Texas Disciplinary

^{1.} Any opinions expressed in this chapter are those of Kathy Owen Brown in her individual capacity and do not reflect any opinion of DLA Piper LLP (US).

Rules of Professional Conduct promotes zealously representing clients: "As a representative of clients, a lawyer performs various functions. . . . As advocate, a lawyer zealously asserts the client's position under the rules of the adversary system."² "In all professional functions, a lawyer should zealously pursue clients' interests within the bounds of the law."³

However, there are limits on zeal. As set forth in the preamble to the rules, zeal must be within the rules of the adversary system and within the bounds of the law. For example, an attorney is not allowed to use tactics in representing a client that have no substantial purpose other than to burden the other party.⁴

The Sedona Conference, well-known for its learned publications and resources on several topics, including e-discovery topics, has issued a "Cooperation Proclamation," which has been endorsed by many judges.⁵ The proclamation's purpose is to launch "a coordinated effort to promote cooperation by all parties to the discovery process to achieve the goal of a 'just, speedy, and inexpensive determination of every action."⁶ This purpose is reflected in the first subtitle in the proclamation: "Cooperation in Discovery is Consistent with Zealous Advocacy."⁷

Cooperation between parties in litigation will result in a significant number of benefits for the parties and the court. First, cooperation will result in more streamlined litigation. By cooperating and having open lines of communication, attorneys will be able to seek and receive a more reasonable volume of data. Parties will not burden the courts as often with discovery hearings. Cooperation does not mean opening up the storehouse and letting the opposition have unfettered access to everything. It means each side having sufficient information about the case and the available data so that they can meaningfully discuss things like data sources, scope, search terms, and predictive coding. Cooperation is often not a one-time discussion, especially in larger matters. As discovery progresses, the parties leave open the option for further discussions, which could broaden or limit the scope of discovery if different information is discovered.

- 3. Tex. Disciplinary R. Prof'l Conduct preamble ¶ 3.
- 4. Tex. Disciplinary R. Prof'l Conduct R. 4.04(a).

- 6. The Sedona Conference, Cooperation Proclamation, at 331.
- 7. The Sedona Conference, Cooperation Proclamation, at 331.

^{2.} Tex. Disciplinary R. Prof'l Conduct preamble ¶ 2.

^{5.} The Sedona Conference, *The Sedona Conference Cooperation Proclamation*, 10 Sedona Conf. J. 331, 334–38 (2009 Supp.).

§ 19.2

Cooperation is a win-win-win for the parties, the clients, and the courts. Although contrary to many styles of practice in recent years, cooperation is becoming more and more crucial as the volume of data continues to grow.

§ 19.2:2 Competence

Almost any attorney would acknowledge that competence is required when representing clients. After all, competence is addressed in the very first rule of the Texas Disciplinary Rules of Professional Conduct and the American Bar Association (ABA) Model Rules of Professional Conduct. A practitioner who focuses on criminal law would likely not represent a party in an oil and gas royalty dispute. Likewise, a practitioner who focuses on antitrust litigation would likely not represent a party in a hotly contested divorce and child custody dispute. Attorneys typically know their limitations in their practice areas. However, attorneys often do not realize their lack of knowledge or competence when it comes to matters of technology and e-discovery.

Texas Disciplinary Rules of Professional Conduct: Rule 1.01 requires that "[a] lawyer shall not accept or continue employment in a legal matter which the lawyer knows or should know is beyond the lawyer's competence, unless: (1) another lawyer who is competent to handle the matter is, with the prior informed consent of the client, associated in the matter⁹⁸ Comment 8 to rule 1.01 was amended in February 2019 by the Texas Supreme Court and specifically includes a technology component. It now reads: "[b]ecause of the vital role of lawyers in the legal process, each lawyer should strive to become and remain proficient and competent in the practice of law, *including the benefits and risks associated with relevant technology*. To maintain the requisite knowledge and skill of a competent practitioner, a lawyer should engage in continuing study and education.⁹⁹

ABA Model Rules of Professional Conduct: Similarly, model rule 1.1 requires that "[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation necessary for the representation."¹⁰ Comment 8 to model rule 1.1, which was amended in 2012 to specifically address technology, advises that "[t] maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing

10. Model Rules of Prof'l Conduct R. 1.1 (Am. Bar. Ass'n. 2019).

^{8.} Tex. Disciplinary R. Prof'l Conduct R. 1.01(a)(1).

^{9.} Tex. Disciplinary R. Prof'l Conduct R. 1.01(a)(1) cmt. 8 (emphasis added).

study and education and comply with all continuing legal education requirements to which the lawyer is subject."¹¹

Competence in E-Discovery: The days have passed when attorneys could avoid having to deal with e-discovery issues by either sticking their heads in the sand or by blaming their lack of knowledge on not being "tech savvy." Attorneys have an ethical duty of competence. Comment 8 to both Texas rule 1.01 and model rule 1.1 make clear that it is not enough that attorneys initially gain knowledge. They must maintain that knowledge. More and more states are amending their disciplinary rules and/or comments to include the language in comment 8 of model rule 1.1 requiring attorneys be competent in technology. As of the date of publication, thirty-six states have a requirement of technological competence in their disciplinary rules or comments.¹²

The 2006 amendments to the Federal Rules of Civil Procedure created new duties and obligations that require lawyers be competent in current technology and adequately prepared. For example, attorneys must—

- 1. even before receipt of a discovery request, advise opposing parties of the description and location of ESI supportive of their clients' claims or defenses;¹³
- 2. confer on any issues related to the disclosure or discovery of ESI;¹⁴ and
- 3. appropriately distinguish between ESI that is reasonably accessible from that which is not.¹⁵

State Bars have continued to emphasize a lawyer's duty to competently handle technological issues related to his or her practice. For example, in 2016 the Supreme Court of Florida amended The Florida Bar Rules to emphasize that "[c]ompetent representation may also involve the association or retention of a nonlawyer advisor of established technological competence in the field in question"¹⁶ and to require that lawyers obtain at least three continuing legal education hours per year from "approved technology programs."¹⁷ North Carolina became the second state to add a

12. See www.lawsitesblog.com/tech-competence.

- 14. Fed. R. Civ. P. 26(f); see also chapter 6 of this book.
- 15. Fed. R. Civ. P. 26(b)(2)(B).
- 16. Rules Regulating The Fla. Bar R. 4-1.1 cmt.
- 17. Rules Regulating The Fla. Bar R. 6-10.3(b).

^{11.} Model Rules of Prof'l Conduct R. 1.1 cmt. 8 (emphasis added).

^{13.} Fed. R. Civ. P. 26(a)(1)(A)(ii).

Ethical Issues in E-Discovery

requirement that attorneys receive technology training. Beginning in 2019, all North Carolina lawyers will be required to complete one hour per year of CLE devoted to technology training.¹⁸

Counsel cannot merely defer to his client to investigate and determine the required information. Instead, counsel shares responsibility with the client for compliance with these obligations.¹⁹ For example, the State Bar of California Standing Committee on Professional Responsibility and Conduct, in Formal Opinion No. 2015-193 (June 30, 2015), warns that "a lack of technological knowledge in handling e-discovery may render an attorney ethically incompetent to handle certain litigation matters involving e-discovery, absent curative assistance under rule 3-110(C), even where the attorney may otherwise be highly experienced."²⁰

Judges are becoming impatient with attorneys who are uninformed about technology and e-discovery issues. United States Magistrate Judge John M. Facciola for the United States District Court for the District of Columbia told an audience at a February 4, 2009, Legal Tech Keynote address that "[w]atching an incompetent lawyer is like watching a clumsy ballerina."²¹ Courts will not excuse an attorney's lack of competence when he makes commitments not understanding the effort and cost involved in keeping the commitment.²² Courts also will not excuse an attorney's lack of knowledge when it results in the attorney providing false and misleading information.²³

Fortunately, competence does not require every attorney to become an information technology expert. But attorneys do need to be able to recognize what they do not know and be willing to associate with persons who have the appropriate technical knowledge and competence to handle those issues for a matter.²⁴

21. Jeff Beard, *Thoughts from Legal Tech 2009*, Lawtech Guru Blog (Feb. 9, 2009) www. lawtechguru.com/archives/legal_technology.html.

22. See In re Fannie Mae Sec. Litig., 552 F.3d 814 (D.C. Cir. 2009).

23. See Peter Kiewit Sons', Inc. v. Wall St. Equity Grp., Inc., No. 8:10CV365, 2012 WL 1852048, at *22 (D. Neb. May 18, 2012).

24. Tex. Disciplinary R. Prof'l Conduct F. 1.01(a)(1); see also State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct Op. 2010-179 (2010).

^{18. 27} N.C.A.C. Chapter 1D § 1518(a)(2).

^{19.} See, e.g., Phoenix Four, Inc. v. Strategic Resources Corp., No. 05 Civ. 4837(HB), 2006 WL 1409413, at *8 (S.D.N.Y. May 23, 2006).

^{20.} State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct Op. 2015-193, p. 7 (June 30, 2015).

§ 19.2:3 Confidentiality

Clients entrust attorneys with information. That information is often personal, sensitive, proprietary, and privileged. Depending on the client, the confidentiality of the information may be subject to confidentiality requirements under state or federal law. As attorneys, we have an obligation to keep nonpublic information entrusted to us as confidential. In this current age of short deadlines, emerging technology, and data security challenges, attorneys must maintain an awareness of their confidentiality obligations.

Texas Disciplinary Rules of Professional Conduct: Rule 1.05(b)(1) states-

- (b) Except as permitted by paragraphs (c) and (d), or as required by paragraphs (e) and (f), a lawyer shall not knowingly:
 - (1) Reveal confidential information of a client or a former client to:
 - (i) a person that the client has instructed is not to receive the information; or
 - (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm.²⁵

A lawyer's obligation to keep client information confidential may, under certain circumstances, determine whether a lawyer communicates with the client electronically. For example, the State Bar of Texas Professional Ethics Committee, in Ethics Opinion No. 648 (April 2015), has outlined a number of factors lawyers should consider before communicating electronically about confidential client information. Extra caution must be given when—

- 1. communicating highly sensitive or confidential information via e-mail or unencrypted e-mail connections;
- 2. sending an e-mail to or from an account that the e-mail sender or recipient shares with others;
- 3. sending an e-mail to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the e-mail account, or to an individual client at that client's work e-mail account, especially if the e-mail

^{25.} Tex. Disciplinary R. Prof'l Conduct R. 1.05(b)(1).

relates to a client's employment dispute with his employer (see ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011));

- 4. sending an e-mail from a public computer or a borrowed computer or where the lawyer knows that the e-mails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
- 5. sending an e-mail if the lawyer knows that the e-mail recipient is accessing the e-mail on devices that are potentially accessible to third persons or are not protected by a password; or
- 6. sending an e-mail if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's e-mail communication, with or without a warrant.²⁶

ABA Model Rules of Professional Conduct: Model rule 1.6(a) requires: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by paragraph (b)."²⁷

In the 2012 amendments to the model rules, the ABA added the following as model rule 1.6(c), which focuses on confidentiality issues in technology. That rule states "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."²⁸

Comment 18 to model rule 1.6, also added in 2012, states-

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See rules 1.1, 5.1, and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to

^{26.} See Tex. Comm. on Prof'l Ethics, Op. 648.

^{27.} Model Rules of Prof'l Conduct R. 1.6(a).

^{28.} Model Rules of Prof¹ Conduct R. 1.6(c); *see also, e.g.*, Iowa State Bar Assoc. Comm. Ethics and Practice Guidelines Ethics Op. 15-01 (Jan. 28, 2015) (stating that a lawyer must "warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, to which a third party may gain access").

prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to forgo security measures that would otherwise be required by this rule.²⁹

Comment 19 to model rule 1.6 states-

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule.³⁰

Confidentiality in E-Discovery: Before getting to high-tech issues, first begin with a low-tech one: attorneys should not have screens from computers, tablets, or smart phones displayed in a way that allows other individuals to read the screen. Attorneys also need to be mindful of who might be able to overhear a conversation. Attorneys should not let others use devices containing confidential client information if that information is not stored on the device in a way that protects it from being accessed by others who might pick up the device (e.g., protected by passwords or encryption). These practices could result in the disclosure of confidential client information.

^{29.} Model Rules of Prof'l Conduct R. 1.6(a) cmt. 18.

^{30.} Model Rules of Prof'l Conduct R. 1.6(a) cmt. 19.

If confidential information is being transferred to third parties in the course of representing a client, attorneys need to ensure that appropriate agreements or orders, such as nondisclosure agreements and confidentiality orders, are in place to protect the transfer of that information. Because there is always the possibility of inadvertent disclosure of confidential or privileged information, if not otherwise provided by the rules applicable to a matter,³¹ an attorney should have a clawback agreement and have that agreement entered as an order by the judge. If an attorney is using the cloud to transmit or store data, special precautions should be taken.³²

§ 19.2:4 Candor

Attorneys must exercise candor before the court. In dealing with e-discovery, the duty of candor goes hand in hand with other ethical obligations, including competence and diligence. Attorneys must be able to understand and communicate the availability of data and any issues related to such data. Attorneys must be diligent in gathering information relating to client data so that they can make accurate representations to the court.

Texas Disciplinary Rules of Professional Conduct: Rule 3.03 provides:

- (b) A lawyer shall not knowingly:
 - (1) make a false statement of material fact or law to a tribunal;
-
- (5) offer or use evidence that the lawyer knows to be false.
- (c) If a lawyer has offered material evidence and comes to know of its falsity, the lawyer shall make a good faith effort to persuade the client to authorize the lawyer to correct or withdraw the false evidence. If such efforts are unsuccessful, the lawyer shall take reasonable remedial measures, including disclosure of the true facts.³³

ABA Model Rules of Professional Conduct: Model rule 3.3 provides:

(b) A lawyer shall not knowingly:

\$ 19.2

^{31.} See, e.g., Tex. R. Civ. P. 193.3(d); Fec. R. Evid. 502.

^{32.} See § 19.3 in this chapter.

^{33.} Tex. Disciplinary R. Prof'l Conduct R. 3.03(a), (b).

- make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;
- (3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.³⁴

Candor in E-Discovery: The duty of candor with the court extends to e-discovery. Violations of this duty can arise by the attorney's making false, misleading, evasive, or incomplete answers to discovery. They can also result from improperly limiting searches for electronic data and failing to disclose destroyed data when there is a duty to do so.

In some instances, an ethical dilemma can arise between an attorney and his client when the client is instructing the attorney to withhold information regarding ESI. Lawyers have a duty to follow the directions of their clients.³⁵ But there are limits on that duty. If the client insists that the attorney engage in conduct that would constitute a fraud on the court, the attorney may have no other option than to withdraw from representation of that client.³⁶

§ 19.2:5 Diligence

Attorneys are required to diligently represent their clients. Diligence applies in many areas of representation, including preservation of electronic data in the client's possession, timely issuing a legal hold, supervising contract attorneys, and vetting third parties to be granted access to client data.

^{34.} Model Rules of Prof'l Conduct R. 3.3(a)(1), (3).

^{35.} Tex. Disciplinary R. Prof'l Conduct R. 1.02(a)(1); Model Rules of Prof'l Conduct R. 1.2(a).

^{36.} Tex. Disciplinary R. Prof'l Conduct R. 1.02(c), (f); 1.15(a); Model Rules of Prof'l Conduct R. 1.2(d), 1.16(a)(1).

Texas Disciplinary Rules of Professional Conduct: Rule 1.01(b) provides, "[i]n representing a client, a lawyer shall not: (1) neglect a legal matter entrusted to the lawyer."³⁷ In defining "neglect," rule 1.01(c) provides, "[a]s used in this rule 'neglect' signifies inattentiveness involving a conscious disregard for the responsibilities owed to a client or clients."³⁸

ABA Model Rules of Professional Conduct: Model rule 1.3 states, "[a] lawyer shall act with reasonable diligence and promptness in representing a client."³⁹

Diligence in E-Discovery: Diligence is very important as it applies to electronic data. The passage of time can result in the loss of data. Courts are finding that the duty to preserve data is arising earlier and earlier in litigation.⁴⁰ Attorneys must be diligent in working with their clients to issue a legal hold and identify all data sources.⁴¹

In large matters with significant amounts of data, attorneys often outsource document review to be able to conduct the review in a quicker and more cost effective manner. However, when using contract attorneys, attorneys must be diligent in supervising the attorneys.⁴² When outsourcing data storage to the cloud, attorneys must be diligent in evaluating the vendors.⁴³

- 37. Tex. Disciplinary R. Prof'l Conduct R. 1.01(b)(1).
- 38. Tex. Disciplinary R. Prof'l Conduct R. 1.01(c).
- 39. Model Rules of Prof'l Conduct R. 1.3.

40. See, e.g., E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc., 803 F. Supp. 2d 469 (E.D. Va. 2011) (finding that defendants' delay of six days in issuing legal hold notice to key employees after learning action had been filed was too long and that notice needed to be in native language of recipients); *Phillip M. Adams & Assoc., LLC v. Dell, Inc.*, 621 F. Supp. 2d 1173, 1191 (D. Utah 2009) (recognizing that preservation duty was triggered when defendant's industry was "sensitized to the issue" in the case and discussing importance of centralized doc.ment retention policies); see also Phillip M. Adams & Assoc., LLC v. Winbond Elecs. Corp., No. 1:05-CV-674 TS, 2010 WL 3767318, at *1 (D. Utah Sept. 16, 2010) (concluding that defendants' duty to preserve was triggered by fact that "[i]n late 1999 the entire computer and component manufacturer's industry was put on notice of a potential for litigation regarding defective floppy disk components ('FDCs') by the well-publicized settlement in a large class action law-suit against Toshiba"). See also chapter 2 in this book.

41. See Phoenix Four, Inc. v. Strategic Resources Corp., No. 05 Civ. 4837, 2006 WL 1409413, at *8 (S.D.N.Y. May 23, 2006) (stating that counsel cannot rely on client's assertions regarding sources and locations of discoverable information without conducting an independent inquiry).

- 42. See § 19.3 in this chapter.
- 43. See § 19.3 in this chapter.

§ 19.3 Applying the Four Cs and the D to Specific Scenarios

§ 19.3:1 Cloud Computing

Cloud solutions for data storage are becoming more and more prevalent. Simply put, the cloud, when referring to electronic data as data storage (which can include servers, networks, applications, and support services), is data maintained by a third party and accessed by an Internet connection. For example, many use an e-mail provider such as Yahoo or Google, and that e-mail is being stored on remote servers and accessed by the individual via an Internet connection. Other common examples of cloud storage are Dropbox, iCloud, and Amazon Cloud. In addition, more and more companies are going to cloud-based solutions for their data storage such as those offered by Microsoft and Google. Many attorneys use e-discovery vendors who process client data and host it on a platform for reviewing, coding, and producing. Some cloud providers allow access to proprietary programs to support needs such as accounting and human resources, in addition to just providing data storage.

There are many reasons individuals and businesses today, including attorneys and their clients, are using cloud solutions for their data needs. Cloud solutions can result in cost savings for the user. The user does not have to pay for internal infrastructure or for the information technology staff to maintain the infrastructure. Cloud providers allow for more scalability of data storage. It is quicker and much easier for a cloud provider, whose business is to provide data storage, to add extra gigabytes or terabytes of data storage. Reputable cloud providers' primary business purpose is the provision of data related storage and services, so they are staffed with professionals trained on the providers' infrastructure. Those cloud providers that include software as part of the cloud services typically have programming specialists to assist their clients. By using a reputable cloud provider, most attorneys and their clients can save costs while gaining more flexibility, scalability, and a higher level of support.

While cloud solutions offer many business advantages, there are ethical factors attorneys must consider before using a cloud solution.

Confidentiality and the Cloud: Before using a cloud solution, it is important to first evaluate the cloud provider's policies on data ownership and data privacy. For example, if the cloud provider receives a subpoena for data, what policies will that subpoena implicate? Usually there is more flexibility and control when using a paid or contracted solution as opposed to a free cloud solution.

Ethical Issues in E-Discovery

Ethical Duty of Confidentiality: As discussed above, attorneys owe a duty of confidentiality to their clients. For example, Texas rule 1.05(b) provides that attorneys cannot disclose confidential information received from a client. Model rule 1.6(a) provides that a lawyer shall not reveal client information unless the client gives informed consent. This rule of professional conduct, considered with attorneys' fiduciary duty to clients, could create an obligation on the part of attorneys to perform an inquiry into the level of security and the potential risk for disclosure of a client's data before placing it on a cloud. However, cloud computing is becoming more accepted as use of the cloud becomes more standard by firms and their clients.⁴⁴

Subpoena Responses: If the cloud provider receives a subpoena for data, what are its policies for complying with that subpoena? Will it notify the individual or company who placed the data on its cloud? Oath's privacy policy (formerly Yahoo) for its free cloud-based services,⁴⁵ as well as Dropbox's privacy policy,⁴⁶ make assurances that the user's data will be kept private. However, both policies state that the providers will comply with subpoenas, court orders, and other such compulsory legal requests. Moreover, there is no indication in either policy that the providers will notify the user of such a request. On the other hand, if an attorney or law firm is paying a cloud provider to provide business solutions, there is often a higher level of user notification when the provider receives third-party requests, such as those described in the terms for the Google, G Suite, Cloud offering.⁴⁷

Cloud Provider Access to Data: Some cloud providers expressly inform users that they access their stored information and cull through that information for their own purposes. Third-party access to the data and how the information obtained is used or disseminated raises confidentiality concerns that should be considered before placing data in the cloud.

Type of Data and Encryption: Attorneys and their clients should be conservative about storing critical data in the cloud. Encrypting data before placing it in the cloud can help. Additionally, if a service-level agreement (SLA) is not in place covering data access and privacy, highly confidential data, such as HIPAA-protected informa-

- 45. Oath Privacy Policy, https://policies.oath.com/us/en/oath/privacy/.
- 46. Dropbox Privacy Policy, Dropbox, www.dropbox.com/privacy.

47. Google Apps for Business (Online) Agreement, Google Apps, https://gsuite.google.com/intl/ en/terms/2013/1/premier_terms.html.

^{44.} See https://abovethelaw.com/legal-innovation-center/2019/04/04/lawyers-and-cloud-computing-its-not-so-complicated-anymore/.

tion, Social Security numbers, credit card information, and intellectual property, should be carefully evaluated before placing it in a cloud.

Competence and the Cloud: As discussed above, lawyers must provide competent representation to their clients. They have obligations to not only maintain knowledge relevant to their practice but to also stay abreast of developments and obtain additional knowledge when needed. Attorneys are very familiar with Tex. Disciplinary Rules Prof²1 Conduct R. 1.01(a)(1). Attorneys must have the knowledge and skill for the representation.

But has anyone considered whether that requirement extends to an ability to evaluate and choose vendors? The ABA has. Comment 8 to model rule 1.1 explains that to "maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology...."⁴⁸

So not only do attorneys have an obligation to keep up with their practice areas, they also need to keep up with technology or hire someone who can do that on their behalf.

Diligence, the Duty to Supervise, and the Cloud: In the context of cloud solutions, diligence and the duty to supervise go hand in hand. In selecting a cloud provider, an attorney should review and understand the provider's policies, practices, and procedures to ensure they are compatible with the lawyer's professional obligations. Then the attorney should use diligence to periodically review and reexamine the provider's policies, practices, and procedures to ensure that they remain compatible with the lawyer's professional obligations.

The standard articulated in many states' ethics opinions is "reasonable efforts" or "reasonable care."⁵⁰

^{48.} Model Rules of Prof'l Conduct R. 1.1 cmt. 8. This language was added in 2012.

^{49.} See, e.g., N.Y. Bar Ass'n Comm. on Prof'l Ethics Op. 842 (Sept. 9, 2010); Iowa State Bar Ass'n Comm. on Ethics and Practice Guidelines, Op. 14-01, at 1–2 (March 10, 2014).

^{50.} See, e.g., Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Op. 2011-200 (2011); N.Y. Bar Ass'n Comm. on Prof'l Ethics, Op. 842 (2010); State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Op. 2010-179 (2010); Wis. State Bar Prof'l Ethics Comm. Formal, Op. EF-12-01 (June 15, 2012).

§ 19.3:2 Document Review

In large matters it is now common for corporations and law firms to outsource their document reviews to contract attorneys. Outsourcing document review can result in substantial cost savings. Although many of these document reviews occur remotely, reviewing attorneys must diligently oversee the review process.

Duty to Supervise: When outsourcing a document review, attorneys must be mindful of their duty to supervise under the applicable ethical rules. Off-site review can provide additional challenges to supervision.

Texas Disciplinary Rules of Professional Conduct: Rule 5.01 states:

A lawyer shall be subject to discipline because of another lawyer's violation of these rules of professional conduct if:

- (b) The lawyer is a partner or supervising lawyer and orders, encourages, or knowingly permits the conduct involved; or
- (c) The lawyer is a partner in the law firm in which the other lawyer practices, is the general counsel of a government agency's legal department in which the other lawyer is employed, or has direct supervisory authority over the other lawyer, and with knowledge of the other lawyer's violation of these rules knowingly fails to take reasonable remedial action to avoid or mitigate the consequences of the other lawyer's violation.⁵¹

Rule 5.03 addresses the duty to supervise nonlawyers:

With respect to a nonlawyer employed or retained by or associated with a lawyer:

- (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
- (c) a lawyer shall be subject to discipline for the conduct of such a person that would be a violation of these rules if engaged in by a lawyer if:

^{51.} Tex. Disciplinary R. Prof'l Conduct R. 5.01.

- (1) the lawyer orders, encourages, or permits the conduct involved; or
- (5) the lawyer:
 - (i) is a partner in the law firm in which the person is employed, retained by, or associated with; or is the general counsel of a government agency's legal department in which the person is employed, retained by or associated with; or has direct supervisory authority over such person; and
 - (ii) with knowledge of such misconduct by the nonlawyer knowingly fails to take reasonable remedial action to avoid or mitigate the consequences of that person's misconduct.⁵²

ABA Model Rules of Professional Conduct: Model rule 5.1 states:

- (b) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.
- (c) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.
- (d) A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:
 - the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or
 - (5) the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.⁵³

^{52.} Tex. Disciplinary R. Prof'l Conduct R. 5.02.
ABA Formal Opinion 08-451 states that although comment 1 to model rule 5.1 paragraph (b) applies to lawyers who have supervisory authority over the work of other lawyers in a firm, the drafters of the rules likely did not intend to restrict the application of rule 5.1(b) to the supervision of lawyers within firms as defined in rule 1.0(c).⁵⁴ Model rule 1.0(c) defines a "firm" or "law firm" as "a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship, or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization."⁵⁵ This rule requires lawyers supervising other lawyers to ensure competent and diligent representation of the client pursuant to model rules 1.1 and 1.3, as well as the protection of a client's confidential information pursuant to model rule 1.6.

Model rule 5.3 also applies to the duty to supervise—

With respect to a nonlawyer employed or retained by or associated with a lawyer:

- (b) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
- (c) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
- (d) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
 - (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
 - (5) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed,

^{53.} Model Rules of Prof'l Conduct R. 5.1

^{54.} ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008).

^{55.} Model Rules of Prof'l Conduct R. 1.0

or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.⁵⁶

The rules impose a higher standard of care for supervising nonlawyer assistants than for supervising subordinate attorneys. The measures employed in supervising nonlawyers should consider the fact that nonlawyers do not have legal training and are not subject to professional discipline.⁵⁷

Guidance from ABA Formal Opinions: ABA Formal Opinion 88-356 (Temporary Lawyers) provides that "[s]upervising lawyers with the firm also have an obligation to make reasonable efforts to ensure that the temporary lawyer conforms to the rules of professional conduct, including those governing the confidentiality of information relating to representation of a client."⁵⁸ Formal opinion 88-356 further notes that "where the temporary lawyer is performing independent work for a client without the close supervision of a lawyer associated with the law firm, the client must be advised of the fact that the temporary lawyer will work on the client's matter and the consent of the client must be obtained."⁵⁹

ABA Formal Opinion 08-451 (Lawyer's Obligations When Outsourcing Legal and Nonlegal Support Services) notes that a lawyer may outsource legal or nonlegal support services provided the lawyer remains ultimately responsible for rendering competent legal services to the client under model rule 1.1, which requires a lawyer to "provide competent representation to a client."⁶⁰ Competent representation "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."⁶¹ The challenges for the outsourcing lawyer include ensuring that tasks are delegated to individuals competent to perform them and overseeing execution of the project adequately and appropriately. Formal opinion 08-451 further states a lawyer outsourcing services for "ultimate provision" to a client should—

61. Model Rules of Prof'l Conduct R. 1.1.

^{56.} Model Rules of Prof'l Conduct R. 5.3.

^{57.} See Model Rules of Prof'l Conduct R. 5.3 cmt 1.

^{58.} ABA Comm. on Ethics & Prof'l Responsibility Formal Op. 88-356 (1988).

^{59.} ABA Comm. on Ethics & Prof'l Responsibility Formal Op. 88-356 (1988) (emphasis added).

^{60.} See ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008).

- 1. conduct reference and background checks of the lawyer or nonlawyer providing the services, as well as any nonlawyer intermediary involved, such as a temporary placement agency or service provider;
- 2. interview principal lawyers, if any, involved in the project;
- 3. inquire into intermediary's hiring practices to evaluate quality and character of the employees likely to have access to the client's information;
- 4. investigate security of the service provider's premises, computer network, and its recycling or refuse disposal procedures;
- 5. conduct a site visit to intermediary's facility; and
- 6. disclose the outsourcing relationship to the client and obtain informed consent from the client.⁶²

When engaging lawyers trained in a foreign country, the supervising lawyer should assess whether the legal education system is comparable to that in the U.S. and evaluate professional regulatory and disciplinary enforcement system for lawyers in that country.

Malpractice Lawsuit Alleging the Failure to Supervise Outsourced Work: In June 2011, a former client filed a malpractice suit in California state court against McDermott Will & Emery (MWE) alleging improper supervision of an e-discovery vendor. J-M Manufacturing complained that MWE failed to supervise properly the e-discovery efforts in response to a whistleblower investigation. According to the complaint, MWE inadvertently produced 3,900 privileged documents that were handed over to the federal government and subsequently to a third party.⁶³ The complaint alleged that MWE's attorneys performed only a limited spot-check of the contract attorneys' document review work and did not perform a thorough review of the privilege categorizations.⁶⁴ This case appears to represent the first time a law firm has been sued for e-discovery malpractice.

^{62.} In formal opinion 88-356, it was concluded that there was no duty to give notice to or obtain consent from a client when hiring a temporary attorney who the engaged attorney would supervise closely. Nevertheless, formal opinion 08-451 recognizes that the prior opinion "was predicated on the assumption that the relationship between the firm and the temporary lawyer involved a high degree of supervision and control, so that the temporary lawyer would be tantamount to an employee" Because the relationship between the firm and contracted personnel is usually more attenuated in an outsourcing situation, it is best practice to give notice and obtain informed consent under those circumstances.

^{63.} J-M Mfg. Co. v. McDermott Will & Emery, No. BC462832, 2011 WL 2296468 (Cal. Super. Ct. June 2, 2011).

^{64.} J-M Mfg., 2011 WL 2296468.

§ 19.3:3 Billing for Contract Attorneys

Supervising lawyers must consider how to bill their clients for work performed by contract attorneys. Billing options include having the contract agency bill the client directly, passing the bills directly to the client, or adding a fee before sending the bill to the client. In deciding how to bill the client, the supervising attorney should consider relevant ethical guidelines.

Texas Disciplinary Rules of Professional Conduct: Rule 1.04(a) provides that a legal fee cannot be illegal or unconscionable, and rule 1.04(b) provides factors to consider in determining reasonableness.

Rule 1.04(f) requires that when a law firm and a lawyer who is not in the firm divide legal fees or agree to do so, the division must meet several requirements, including: (1) either the billing is in proportion to services performed or the lawyers involved assume joint responsibility for the matter, (2) the client consents in writing to the terms of the fee division arrangement, and (3) the total fee complies with the requirement of rule 1.04(a) that a fee for legal services not be unconscionable.⁶⁵

ABA Model Rules of Professional Conduct: Model rule 1.5(a) prohibits a lawyer from charging or collecting an unreasonable fee and includes a series of factors to be considered in determining the reasonableness of a fee.⁶⁶

Guidance from Texas Ethics Opinion No. 577: If a lawyer is in the law firm that is billing for the lawyer's work, such billing will not involve a division of fees and the requirements of rule 1.04(f) will not apply.

The Professional Ethics Committee of the Supreme Court of Texas, in Ethics Opinion No. 577 (March 1, 2007), lists several objective factors to be used to determine whether a lawyer who is not a partner, shareholder, or associate of the firm is or is not in a law firm. They include—

- 1. the receipt of firm communications;
- 2. inclusion in firm events;

^{65.} See Tex. Disciplinary R. Prof'l Conduct R. 1.04(f). A division of fees is a single billing to a client covering the fee of two or more lawyers who are not in the same firm. Tex. Disciplinary R. Prof'l Conduct R. 1.04 cmt. 10. A division of a fee based on the proportion of services rendered by two or more lawyers contemplates that each lawyer is performing substantial legal services on behalf of the client with respect to the matter. Tex. Disciplinary R. Prof'l Conduct R. 1.04 cmt. 12.

^{66.} See Model Rules of Prof'l Conduct R. 1.5(a).

- 3. work location;
- 4. length and history of association with the firm;
- 5. whether the firm and the lawyer identify or hold the lawyer out as being in the firm to clients and to the public; and
- 6. the lawyer's access to firm resources including computer data and applications, client files, and confidential information.⁶⁷

Guidance from ABA Formal Ethics Opinions: ABA Formal Opinion 00-420 (Surcharge to Client for Use of a Contract Lawyer) provides that a law firm that engages a contract lawyer may add a surcharge to the cost paid by the billing lawyer provided the total charge represents a reasonable fee for the services provided to the client.⁶⁸ In the absence of an understanding to the contrary with the client, if the legal services of a contract lawyer are billed to the client as an expense or cost, the client may be charged only the cost directly associated with the services, including expenses incurred by the billing lawyer to obtain and provide the benefit of the contract lawyer's services. Formal opinion 00-420 further notes that an attorney may bill the contract attorney's charges to the client as fees rather than costs when "the client's reasonable expectation is that the retaining lawyer has supervised the work of the contract lawyer or adopted that work as her own."⁶⁹

In *Carlson v. Xerox Corp.*,⁷⁰ the court employed a lodestar calculation of reasonable attorney's fees and concluded that, if the evidence showed that contract attorneys conducting document review were trained and their work was monitored and reviewed, they were properly supervised and thus the calculation was not inflated by the court's use of a rate of \$300 per hour, even though the contract attorneys were allegedly paid only \$55 per hour.

ABA Formal Opinion 93-379 (Billing for Professional Fees, Disbursements, and Other Expenses) notes that if a firm decides to pass the costs through to the client as a disbursement, no surcharge is permitted.⁷¹ In this situation, the lawyer may bill the cli-

^{67.} See Tex. Comm. on Prof'l Ethics, Op. 577.

^{68.} ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 00-420 (2000).

^{69.} In re Wright, 290 B.R. 145, 153 (Bankr. C.D. Cal. 2003) (citing ABA Formal Opinion 00-420); see also In re Enron Sec., Derivative & ERISA Litig., 586 F. Supp. 2d 732, 783 (S.D. Tex. 2008) (citing In re Wright and ABA Formal Opinion 00-420 in the context of calculating reasonable award of attorneys' fees and noting that there is "not much case law addressing the question [of] whether the charges of contract lawyers and paralegals may be billed separately as attorney's fees at a higher rate than the law firm pays them").

^{70. 596} F. Supp. 2d 400, 410 (D. Conn. 2009).

§ 19.3

ent only its actual cost plus a reasonable allocation of associated overhead, such as the cost of office space, support staff, equipment, and supplies for the individuals under contract. Formal opinion 93-379 also notes that if a lawyer receives a discounted rate from a third-party provider, "it would be improper if she did not pass along the benefit of the discount to her client"

§19.3:4 Metadata

Metadata, widely defined as "data about data," is an often misunderstood but important part of e-discovery. The definition of metadata is far more complex than just "data about data." There are several types of metadata, including application metadata, document metadata, e-mail metadata, and embedded metadata.⁷² The multifacets of metadata create ethical issues for attorneys.

Cooperation: Due to the many issues involved with metadata, including the many options for production of metadata, it is best if the parties can come to an agreement on what metadata fields will be produced. Often in litigation, lawyers may receive requests for "all metadata," but that is seldom what the requesting party is really seeking. A request for all metadata typically is an indicator that an attorney does not understand what metadata is. If a party receives a request for all metadata, it is very important to respond to that request, either in the form of a request for clarification, a proposed agreement on the metadata to be provided, or an objection if the requesting party will not narrow the request. If a party does not respond to a request for all metadata, discovery battles can result if the responding party does not produce all metadata.

When propounding discovery that asks for metadata, be sure that you are not requesting metadata that you would not be willing to provide on behalf of your own client. The adage of "what is good for the goose is good for the gander" applies in discovery. Very often, a requesting party will see the same requests turned around and sent back to him.

^{71.} See ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 93-379 (1993).

^{72.} For a discussion of the importance of metadata in discovery and also an explanation of the different types of metadata, see The Sedona Conference, *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* (2d ed. 2007), https:// thesedonaconference.org/sites/default/files/publications/The%20Sedona%20Principles%20Third %20Edition.19TSCJ1.pdf. For a more detailed discussion of metadata, including definitions, see The Sedona Conference, The Sedona Conference Glossary: E-Discovery & Digital Information Management (3d ed. 2010), https://thesedonaconference.org/publication/The_Sedona_Conference_Glossary; see also Aguilar v. Immigration & Customs Enforcement Div. of U.S. Dep't of Homeland Sec., 255 F.R.D. 350, 353-55 (S.D.N.Y. 2008).

Ethical Issues in E-Discovery

To simplify discovery and to avoid any confusion, it is best for the parties to cooperate on the metadata fields to be provided. The agreement can be set forth in a rule 11 agreement⁷³ or a format of production order.

Competency: As discussed above, attorneys must maintain competence. The duty to maintain previously competence applies to an attorney's area of practice as well as technology.⁷⁴ When handling discovery involving ESI (which is all discovery for all intents and purposes), attorneys must have sufficient competency in understanding metadata—what it is, how to preserve it, how to collect it, what to request, and what to produce. Failure to understand those areas of data could result in harm to the client.

If metadata is not preserved, either by not instructing a client to preserve or by collecting data in such a way that metadata is changed or destroyed, a party (or an attorney) could face sanctions for spoliation (or a potential malpractice claim from the client).

Confidentiality: As discussed above, attorneys have an ethical duty to maintain confidentiality. This duty extends to metadata, which can contain confidential or privileged information. For example, some information that is included in metadata could be track changes or deleted data that contains a comment from an attorney. When producing data, it is important to make sure metadata is also reviewed so that confidential information can be appropriately designated for production pursuant to a protective order and privileged information can be withheld or redacted.

The Texas Disciplinary Rules of Professional Conduct requires lawyers to take reasonable measures to avoid the transmission of confidential information that is embedded in electronic documents.⁷⁵ Whether or not the lawyer took reasonable steps will be a factual determination.⁷⁶ Accordingly, it is important to document the steps taken to prevent the production of confidential information in metadata so that a lawyer can establish that reasonable steps were taken to prevent the inadvertent disclosure.

§ 19.4 Using Social Networking Sites: An Issue for Lawyers, Judges, and Jurors

Careless use of social networking sites like Facebook can create serious problems for litigants, and even lead to a miscarriage of justice in certain circumstances. As offi-

76. Tex. Comm. on Prof'l Ethics, Op. 665.

^{73.} Tex. R. Civ. P. 11.

^{74.} Model Rules of Prof'l Conduct R. 1.1 cmt. 8.

^{75.} Tex. Comm. on Prof'l Ethics, Op. 665.

cers of the court, lawyers should always be cognizant of the ways their use of social media during litigation could affect their clients, the opposing parties, and court proceedings. Likewise, judges have an obligation to refrain from using social media in a way that jeopardizes the integrity of the judicial process. Additionally, judges and

lawyers must ensure that jurors don't use social media in ways that could taint or delay court proceedings.⁷⁷

§ 19.4:1 Limitations for Lawyers

The Texas Disciplinary Rules of Professional Conduct limit lawyers' use of social networking sites to comment on pending litigation. A social media misstep could conflict with a lawyer's duty to competently represent the client's interests to the best of his or her ability, as required by rule 1.01,⁷⁸ or violate a lawyer's duty under rule 1.05 to keep client information confidential.⁷⁹ However, using social media also significantly implicates the rules requiring lawyers to exhibit fairness in court proceedings.

Texas Disciplinary Rule of Professional Conduct 3.04 (Fairness in Adjudicatory Proceedings) provides that "[a] lawyer shall not . . . engage in conduct intended to disrupt the proceedings."⁸⁰

Rule 3.05 (Maintaining Impartiality of Tribunal) states-

A lawyer shall not:

- (b) seek to influence a tribunal concerning a pending matter by means prohibited by law or applicable rules of practice or procedure;
- (c) except as otherwise permitted by law and not prohibited by applicable rules of practice or procedure, communicate or cause another to communicate ex parte with a tribunal for the purpose

^{77.} For a more in-depth discussion of social media obligations in litigation, see chapter 20.

^{78. &}quot;Having accepted employment, a lawyer should act with competence, commitment and dedication to *the interest of the client* and with zeal in advocacy upon the client's behalf." Tex. Disciplinary R. Prof'l Conduct R. 1.01 cmt. 6 (emphasis added).

^{79.} Tex. Disciplinary R. Prof'l Conduct R. 1.05(b) ("[A] lawyer shall not knowingly: (1) Reveal confidential information of a client or a former client to: (i) a person that the client has instructed is not to receive the information; or (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm.").

^{80.} Tex. Disciplinary R. Prof'l Conduct R. 3.04(c)(5).

of influencing that entity or person concerning a pending matter other than:

- (1) in the course of official proceedings in the cause;
- (5) in writing if he promptly delivers a copy of the writing to opposing counsel or the adverse party if he is not represented by a lawyer;
- (5) orally upon adequate notice to opposing counsel or to the adverse party if he is not represented by a lawyer.⁸¹

Rule 3.06 (Maintaining Integrity of Jury System) provides that "[a] lawyer shall not ... seek to influence a venireman or juror concerning the merits of a pending matter by means prohibited by law or applicable rules of practice or procedure."⁸²

Rule 3.07 (Trial Publicity) states-

In the course of representing a client, a lawyer shall not make an extrajudicial statement that a reasonable person would expect to be disseminated by means of public communication if the lawyer knows or reasonably should know that it will have a substantial likelihood of materially prejudicing an adjudicatory proceeding.⁸³

§ 19.4:2 Application of the Texas Disciplinary Rules of Professional Conduct to Social Media Use

The commentary to rule 3.04(c) explains that "[t]he obligations imposed by [paragraph (c)] to avoid seeking to influence the outcome of a matter by introducing irrelevant or improper considerations into the deliberative process are important aspects of a lawyer's duty to maintain the fairness and impartiality of adjudicatory proceedings."⁸⁴ This obligation exists inside and outside the courthouse, and on social networking sites, as rule 3.07 governing extrajudicial statements makes clear.

Rule 3.05 prohibits lawyers from communicating with judges for the purpose of influencing pending litigation. This is a special concern in the social media context where judges and lawyers may be Facebook friends. As will be discussed further in section

^{81.} Tex. Disciplinary R. Prof'l Conduct F. 3.05.

^{82.} Tex. Disciplinary R. Prof'l Conduct R. 3.06(a)(2).

^{83.} Tex. Disciplinary R. Prof'l Conduct F. 3.07(a).

^{84.} Tex. Disciplinary R. Prof'l Conduct F. 3.04 cmt. 4.

19.4:3, some states have issued ethics opinions that clarify the circumstances in which lawyers and judges can "friend" each other and communicate on Facebook.⁸⁵

Along the same lines, the commentary to rule 3.06 explains that "jurors should be protected against extraneous influences" and that "[t]here should be no extrajudicial communication with veniremen prior to trial or with jurors during trial or on behalf of a lawyer connected with the case."⁸⁶ The ABA has taken a similar approach, explaining that a lawyer may review a juror's or potential juror's Internet presence, which may include postings by the juror or potential juror, in advance of and during a trial, but a lawyer may not communicate directly with a juror or potential juror.⁸⁷ Improper communication includes sending an access request to a juror's electronic social media, either personally or through another.⁸⁸ The ABA has also taken the position that a lawyer must take reasonable remedial measures including, if necessary, disclosure to the tribunal if the lawyer discovers social media evidence of juror or potential juror misconduct that is criminal or fraudulent.⁸⁹

Lawyers' misuse of social media can have significant ramifications in the course of legal proceedings. In Minnesota, a Somali man convicted of murder filed a motion for a new trial based on prosecutor's anti-Somali Facebook posts allegedly made during his murder trial. The postings also allegedly contained statements regarding the prosecutor's impressions of one of the jurors in the case.⁹⁰ Although that defendant's motion for a new trial was denied, the case nevertheless demonstrates the risk of jeopardizing the finality of jury verdicts with offensive Facebook posts.

Lawyers should never let their use of social media cost them credibility with the court to the disadvantage of their clients. For example, some states have concluded that lawyers may respond to a former client's negative online review so long as the lawyer's response does not reveal any privileged or confidential information.⁹¹

87. ABA Formal Ethics Op. 466, at 3-6 (Apr. 24, 2014).

- 88. ABA Formal Ethics Op. 466, at 3-6 (Apr. 24, 2014).
- 89. ABA Formal Ethics Op. 466, at 3-9 (Apr. 24, 2014).

90. Debra Cassens Weiss, *Defendant Cites Prosecutor's Facebook Comments in Bid for New Trial*, ABA Journal (Feb. 18, 2010), www.abajournal.com/news/article/defendant_cites_prosecutors_facebook_comments_in_bid_for_new_trial/.

91. See N.Y. Bar Ass'n Comm. on Prof'l Ethics Op. 1032, 1–16 (Oct. 30, 2014); Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility Op. 2014-200, at 6.

^{85.} See § 19.4:3.

^{86.} Tex. Disciplinary R. Prof'l Conduct R. 3.06 cmt. 1.

§ 19.4

Lawyers should also ensure that their clients carefully consider their social media presence before and during litigation, so long as removal of postings will not result in spoliation.⁹² In Texas, a lawyer requested a continuance due to the death of her father, but the lawyer's recent Facebook status told a story of a week filled with drinking and partying.⁹³ Also in Texas, a lawyer complained about a judge's handling of a motion on her Facebook page. The judge "zinged" her back, on Facebook.⁹⁴

§ 19.4:3 Judges' Use of Social Media

Judges' use of social media directly implicates the rule set forth in canon 2 of the Texas Code of Judicial Conduct that requires judges to promote the public's confidence in an impartial judiciary by avoiding any actual impropriety and the appearance of impropriety or improper influence. It also implicates canon 3, and in particular, the rule prohibiting judges from participating in ex parte communications with counsel.

Canons 2 and 3 of the Texas Code of Judicial Conduct: Canon 2 (Avoiding Impropriety and the Appearance of Impropriety in All of the Judge's Activities) states:

- (A) A judge shall comply with the law and should act at all times in a manner that promotes public confidence in the integrity and impartiality of the judiciary.
- (B) A judge shall not allow any relationship to influence judicial conduct or judgment. A judge shall not lend the prestige of judicial office to advance the private interests of the judge or others; nor shall a judge convey or permit others to convey the impression that they are in a special position to influence the judge. A judge shall not testify voluntarily as a character witness.
- (C) A judge shall not knowingly hold membership in any organization that practices discrimination prohibited by law.⁹⁵

Text of canon 3 (Performing the Duties of Judicial Office Impartially and Diligently) provides:

^{92.} See, e.g., Fla. Bar Ass'n, Prof'l Ethics Op. 14-1 (June 25, 2015).

^{93.} Molly McDonough, *Facebooking Judge Catches Lawyer in Lie, Sees Ethical Breaches #ABA-Chicago*, ABA Journal (Jul. 31, 2009), www.abajournal.com/news/article/ facebooking_judge_catches_lawyers_in_lies_crossing_ethical_lines_abachicago/.

^{94.} See McDonough, Facebooking Judge Catches Lawyer in Lie.

^{95.} Tex. Code Jud. Conduct, canon 2.

A judge shall accord to every person who has a legal interest in a proceeding, or that person's lawyer, the right to be heard according to law. A judge shall not initiate, permit, or consider ex parte communications or other communications made to the judge outside the presence of the parties between the judge and a party, an attorney, a guardian or attorney ad litem, an alternative dispute resolution neutral, or any other court appointee concerning the merits of a pending or impending judicial proceeding.⁹⁶

Abiding by Canons 2 and 3 in the Social Media Context: Judges face the same obligations under canons 2 and 3 when using social media as they do when using other forms of communication. In applying similar provisions in the Model Code of Judicial Conduct, the ABA concluded that "judges' use of [social networking] does not necessarily compromise their duties under the Model Code any more than use of traditional and less public forms of social connection such as U.S.P.S. mail, telephone, e-mail or texting."⁹⁷ Nevertheless, because information posted on social networking sites can potentially reach tens of thousands of members of the public, the misuse of social media is especially damaging to the public's trust in the judiciary.

Although Texas has not issued any ethics opinions directly addressing a judge's use of social media, several other states have. According to the Florida Judicial Ethics advisory committee, a judge may not add lawyers who may appear before the judge as "friends" on a social networking site or permit such lawyers to add the judge as their friend.⁹⁸ That rule aims to prevent the appearance of impropriety, so the public does not get the impression that the judge's Facebook friend has special influence over the judge.

The South Carolina Advisory Committee on Standards of Judicial Conduct has reached a more lenient conclusion about whether judges and lawyers can be Facebook friends. It opined that a judge may be a member of Facebook and be friends with law enforcement officers and employees of the magistrate as long as they do not discuss anything related to the judge's position as magistrate.⁹⁹

^{96.} Tex. Code Jud. Conduct, Canon 3.B(8).

^{97.} ABA Formal Ethics Op. 462, at 4 (Feb. 21, 2013).

^{98.} No "Friends" for Judges, Legal Profession Blog (Dec. 8, 2009), https://lawprofessors. typepad.com/legal_profession/2009/12/the-florida-judicial-ethics-advisory-commission-opines-onjudges-use-of-on-line-social-networking-a-summary-of-the-opinion.html.

^{99.} South Carolina Judiciary Department, Advisory Op. No. 17-2009, https://sccourts.org/ advisoryOpinions/html/17-2009.pdf.

Ethical Issues in E-Discovery

One widely publicized case example in Texas illustrates how a judge's abuse of social media during trial can erode the public's trust in the judiciary. During the trial of a criminal case, a judge sent texts to a prosecutor suggesting lines of questioning.¹⁰⁰ On October 21, 2013, the Texas State Commission on Judicial Conduct announced that the judge was stepping down from the bench to avoid disciplinary action.¹⁰¹ Although this example did not involve use of a social media site, the judge's ex parte communications would have been equally improper if made on Facebook through posts or private messages to a lawyer appearing before the judge.

§ 19.4:4 Setting Limits for Jurors

Because the integrity of the judicial process depends in large part on protecting jurors from improper influences, judges and lawyers must take whatever steps they can to minimize the risk that a jury pool will be tainted by information on social networking sites. Some case examples about jurors' use of social media demonstrate the importance of making crystal clear to the jury panel their obligation to refrain from using social media while serving jury duty. Jurors should also be advised of the ramifications on the trial proceedings if they violate that obligation-potential trial delays and appeals from their verdicts.

In a multimillion-dollar civil action in Cincinnati, Ohio, plaintiffs' counsel discovered that a member of the jury pool listed his status update on Facebook as "sitting in hell 'aka jury duty[.]" The judge removed the juror from the jury pool but denied the defendant's motion for a mistrial.¹⁰²

In one Pennsylvania case, a juror used Twitter, Facebook, and blogs to post information about the trial during deliberations, prompting the defendant, a former state senator, to appeal his convictions on 137 counts of fraud, tax evasion, and obstruction of justice.¹⁰³ The court found that the juror violated the court's admonition against dis-

^{100.} Martha Neil, Judge Texted During Trial to Help State, Ex-Prosecutor Says, ABA Journal (July 9, 2013), www.abajournal.com/news/article/judge_texted_during_trial_to_help_state_says_ex -prosecutor/.

^{101.} Cindy Horswell and Brian Rogers, *East Texas Judge Resigns Amid Texting Probe*, Houston Chronicle (Oct. 22, 2013), www.houstonchronicle.com/news/houston-texas/houston/article/East -Texas-judge-resigns-amid-texting-probe-4914820.php.

^{102.} Kimball Perry, Juror Booted for Facebook Comment, Dayton Daily News (Feb. 1, 2009), http://content.hcpro.com/pdf/content/228698.pdf, at A6.

^{103.} United States v. Fumo, 655 F.3d 288 (3rd Cir. 2011) (affirming district court's denial of defendant's motion for new trial).

cussing the details of the trial but that there was no evidence showing that his extrajury misconduct had a prejudicial impact on the verdict.

§ 19.5 Conclusion

As technology and e-discovery evolves, the ethical standards require that attorneys also evolve in their knowledge and practice. Attorneys' duties of competence, confidentiality, candor and diligence require attorneys to keep up with developments and to also have knowledge of clients' systems and data. The trends requiring cooperation will hopefully relieve some of the costs and burdens of e-discovery for all parties involved.

As social media use becomes more and more of a part of our everyday life, attorneys should be mindful of the Texas Disciplinary Rules of Professional Conduct. For example, if one always honors the baseline duty to maintain the impartiality and integrity of court proceedings, abiding by the applicable rules of conduct are really just a matter of common sense and thinking before posting.

In summary, if the conduct would be an ethical violation in a low-tech world, the conduct will also be a violation in a high-tech world.

§ 19.6 Additional Resources

Additional information about ethical issues in e-discovery may be found at the following websites.

- www.edrm.net
- www.ediscoverylaw.com
- www.craigball.com
- www.e-discoveryteam.com
- http://bowtielaw.com/
- www.thesedonaconference.org (including publications)
- www.law.uh.edu/libraries/ethics/homepage.html
- https://www.legalethicstexas.com/
- http://tyla.org/ (Project—TYLA Pocket Guide: Social Media 101)

Chapter 20

Social Media

Justice John G. Browning

§ 20.1 Introduction

Social networking platforms like Facebook, Twitter, YouTube, and LinkedIn have revolutionized the way people communicate and share information. Facebook boasts over 1.2 billion users worldwide, and one out of every seven online minutes is spent on Facebook. Twitter, with over 213 million active users, has gone from processing 5,000 tweets a day in 2007 to over 400 million daily in 2013. According to the Pew Institute, seventy-two percent of all adult Americans maintain at least one social networking profile. And with social media use by society in general at an all-time high, it's hardly surprising that use by lawyers is steadily rising as well. According to a 2012 survey by American Lawyer Media, nearly seventy-five percent of U.S. law firms employ one or more social networking platforms for marketing purposes. But lawyers are finding that sites like Facebook and Twitter are more than just marketing tools; with people seemingly sharing every last detail of their lives online, lawyers in virtually all practice areas have found social media to be a valuable avenue for discovery. The 2012 ABA Legal Technology Survey indicates that at least forty-four percent of lawyers acknowledge making use cf social networking sites for case investigation and discovery.

Texas lawyers, like their counterparts across the country, are experiencing the many different ways in which social networking has impacted the legal system. In virtually all areas of practice—from criminal law to employment law and family law to personal injury cases and commercial litigation—attorneys in Texas are making use of content from social media sites. In Texas, as they have nationwide, social media sites are influencing cases from the very earliest stages of serving a party and determining jurisdiction through to the instructions given to jurors. Texas lawyers must take social media content into consideration not only when it comes to discovery and evidentiary issues, but also such considerations as the online conduct of jurors, lawyers, and even judges. While Texas hasn't yet become "ground zero" for questions about social networking discovery in the sense that a state like Pennsylvania has, as this chapter will demonstrate Texas courts have contributed more than their share to the ever-evolving saga of social media's paradigm-shifting impact on the legal system.

§ 20.2 Discovery of Social Media Content

With seventy-two percent of adult Americans maintaining at least one social networking profile, and with use of social media at ever-growing rates, it is certainly not surprising that attorneys have discovered the litigation value of information contained in a party's postings on social media sites like Facebook and Twitter. But regardless of what a lawyer or party may be able to discover informally on a publicly viewable profile, formal requests for this information must still conform to traditional discovery rules. Recent decisions nationwide confirm that while, generally, objections based on privacy concerns are likely doomed from the start, the availability of social media content does not open the door to a fishing expedition. While there are cases in which a party has been compelled to turn over her entire profile or even produce her social networking password and login credentials, the trend among courts nationally is to refrain from such unfettered discovery.¹ Just because information has been posted on Facebook or Twitter and may be relatively easily produced doesn't mean that standards are relaxed when it comes to requests that are overly broad or seek information that is neither relevant nor reasonably calculated to lead to the discovery of admissible evidence.

For example, requests for a party's entire social networking profile's content, or alternatively that party's Facebook password, are usually going to be viewed as overly broad. Courts have held that while content on a social networking site is discoverable, the discovering party is not entitled to "rummage at will through its opponent's Facebook profile."² A party seeking discovery will still have the burden of showing that the information sought is relevant. In many jurisdictions, this comes down to establishing a factual predicate—some reason to believe that the private portion of a profile contains information relevant to the case. Court after court has rejected a blanket request for "all social media content" or a request that rests on some hope of relevant evidence. Instead, parties seeking discovery should have some basis for a belief that privacy-restricted portions of a profile will contain information relevant to the litigation. "Absent such a showing, [defendant] is not entitled to delve carte blanche into the nonpublic sections of plaintiffs' social networking accounts."³ In many instances, it is information that is publicly viewable and that contradicts some aspect of the

^{1.} See, e.g., John G. Browning, With "Friends" Like These, Who Needs Enemies? Passwords, Privacy, and the Discovery of Social Media Content, 36 Am. J. Trial Advocacy 505 (2013); John G. Browning, Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites, SMU Sci. & Tech. L. Rev., vol. 14, 3, 465 (Summer 2011).

^{2.} See, e.g., Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387, 388 (E.D. Mich. 2012).

^{3.} Keller v. Nat'l Farmers Union Prop. & Cas. Co., No. CV 12-72-M-DLC-JCL, 2013 WL 27731, at *4 (D. Mont. Jan. 2, 2013).

party's claims or defenses that forms the basis for such a predicate. For example, in one personal injury case, the defendant's motion to compel was granted when the plaintiff's claims that he "never [wore] shorts because he [was] embarrassed by his scar," were contradicted by photos on his Facebook and MySpace pages depicting him in shorts.⁴ In other cases, it may be "plaintiff's own testimony at his deposition as to the alleged impact of the claimed accident and his alleged injuries" that establishes a basis for compelling the production of Facebook content.⁵

Moreover, even in cases where what is sought is clearly relevant to some aspect of the party's claims or defenses—such as discovery seeking social media content demonstrative of the party's emotional state in a case where emotional distress is alleged-courts may still rein in discovery. For example, in one employment discrimination case where emotional distress was alleged, the defendant sought any social media content that "reveals or relates to plaintiff's emotion, feeling, or mental state." The court held that was too broad, and crdered the plaintiff to produce any posts that "reveal, refer, or relate to . . . any significant emotion, feeling, or mental state allegedly caused by defendant's conduct."⁶ Parties on both sides are invariably better off propounding more narrowly tailored discovery requests when seeking social media content, as opposed to sending overly broad requests, seeking the entire contents of a social networking profile, asking for a Facebook password, or similarly unrestricted access to a profile.

Unlike states like Pennsylvania or New York (which have been hotbeds of judicial activity related to issues pertaining to the discoverability of social media content), Texas courts have been relatively silent on the subject. Only two reported appellate decisions have confronted the issue of discoverability of social networking evidence. In one, defendants in an underlying personal injury case sought to obtain, via depositions on written questions directed to both Facebook and MySpace, plaintiff Cody Karl's social networking profile contents and to compel the continuation of his deposition until such documents were produced. The trial court granted plaintiff's motion to quash and denied the motion to compel, prompting a mandamus action. In a one-sentence per curiam opinion that sheds no light whatsoever on the reasoning behind it, Houston's First District Court of Appeals denied the petition for writ of mandamus.⁷

^{4.} Zimmerman v. Weis Markets, Inc., Nc. CV-09-1535, 2011 WL 2065410 (Pa. Com. Pl. May 19, 2011).

^{5.} Bianco v. North Fork Bancorporation, Inc., No. 107069/2010, 2012 WL 5199007 (N.Y. Sup. Ct. Oct. 10, 2012).

^{6.} Robinson v. Jones Lang Lasalle Americas, Inc., No. 3:12-cv-00127-PK, 2012 WL 3763545, at *2 (D. Ore. Aug. 29, 2012); see also Mailhoit v. Home Depot U.S.A., Inc., 285 F.R.D. 566 (C.D. Cal. 2012).

In the other case, the discovery dispute came in a wrongful death/medical malpractice action in which the surviving family members were asked to produce copies of any social media postings that pertained to the decedent, Arthur Lowe, or to his death. The plaintiffs objected, calling the request "an invasion of privacy and any such information would be unreliable and constitute hearsay and a fishing expedition and this request is meant for the purpose of harassment." The trial court denied the hospital's motion to compel, but there was no reporter's record of the hearing. The appellate court found that the requests seeking posts about the decedent before he died were not limited in time and that the requests for the social networking posts should have been more limited in time. While the court explicitly rejected the plaintiff's arguments as to privacy and found that they would be clearly relevant to the issue of mental anguish, nevertheless, the court concluded that "a request without a time limit for posts is overly broad on its face."⁸ Consequently, it held that the trial court's denial of the defendant's motion to compel was not an abuse of discretion.

The paucity of reported Texas case law on discovery issues involving social media will no doubt end as use of social networking content becomes more widespread and discovery disputes naturally follow. In the meantime, the lessons learned from the Christus Health case are consistent with trends that can be observed from courts around the country. Privacy objections are largely futile,⁹ and relevant social media content should be produced in response to narrowly tailored discovery requests that are limited in time and scope of what is being sought.¹⁰

§ 20.3 Attempts to Secure Social Media Directly from a Social Media Site Are Generally Futile

Social media sites like Facebook have their own policies and procedures for requesting personal information about their users. Facebook's stated policy is that the Stored Communications Act prohibits any disclosure by Facebook of user content. Facebook instructs parties to a litigation to produce and authenticate the contents of their own accounts by downloading the information from the account.

^{7.} In re Magellan Terminals Holdings, L.P., No. 01-11-00373-CV, 2011 WL 2150422, at *1 (Tex. App.—Houston [1st Dist.] May 13, 2011, orig. proceeding) (mem. op.).

^{8.} In re Christus Health Southeast Texas, 399 S.W.3d 343 (Tex. App.-Beaumont 2013).

^{9.} Abraham v. Cavender Boerne Acquisition of Texas, Ltd., No. SA-10-CA-453-XR, 2011 WL 13127173 (W.D. Tex. Apr. 26, 2011).

^{10.} In re Indeco Sales, Inc., No. 09-14-00405-CV, 2014 WL 5490943 (Tex. App.—Beaumont Oct. 30, 2014) (requests for social media held to be overly broad).

Instead of attempting to subpoen websites directly, it is simpler to request social media activity through discovery from the party who controls the account. A narrowly tailored request to the party controlling the account should be more effective than attempting to subpoen the website directly.

§ 20.4 Litigant's Duty to Preserve Social Media

Data on social media platforms is subject to the same duty to preserve as other types of relevant evidence. The duty to preserve is triggered when a party reasonably fore-sees that evidence may be relevant to issues in litigation. See chapter 1.

It is important to capture all the related data, not just a copy of a potentially incriminating page. Social media files consist of more than just posts; they consist of related links, videos, embedded files, and metadata. For this reason, although screenshots are commonly used in social media discovery, they may be insufficient in that they capture none of the metadata or associated content. In addition, it is important to know how to harness the information on the social networking web to enhance the ability to obtain admissible social media evidence for trial.

Facebook instructs users on how to preserve Facebook posts. Clients need to understand and use the settings in Facebook. Facebook offers the ability to "Download Your Info." With just one click of the mouse, users can download a ZIP file containing timeline information, posts, messages, and photos. The account holder should go into "Settings" on their Facebook account and navigate to the "Backup" menu. The account holder can preserve the complete history and entire content of the account up to that point in time. Under "Settings," there is an option to "Download a copy of your Facebook data." The account holder will be provided with a link to the archive for the account. Twitter operates in a similar way. This will provide protection from hacking or bogus posts. Information that is not available by merely logging into an account also is included, such as the ads on which the user has clicked, IP addresses that are logged when the user accesses his or her Facebook account, and other potentially relevant information. The downloaded archive may not provide all of the Facebook account, however. Postings made from a mobile device may not show up. Also, information that has been deleted from the account will not be revealed.

Twitter offers a similar, although somewhat limited, option. Twitter users can download all tweets posted to an account by requesting a copy of the user's Twitter archive. Twitter does not, however, offer users a self-serve method of obtaining other, nonpublic information, such as IP logs. To obtain this additional information, users must request it directly from Twitter by sending an e-mail to **privacy@twitter.com** with the subject line, "Request for Own Account Information." Twitter will respond to the e-mail with further instructions.¹¹

§ 20.5 Tools to Capture and Preserve Social Media

Any social media archive needs to be captured and managed in a forensically complete, searchable, and usable format. An archive that includes all original unaltered source files including HTML, images, video, JavaScript, linked files such as PDFs, and any other data referenced or linked to the page will provide the best possible preserved copy of any given page. A program that captures content in real time preserves the most accurate copy possible, since content is being updated, changed, or deleted on an ongoing basis. A failure to catch those changes misses vital information or evidence.

Some available programs include X-1 Social Discovery and Nextpoint. X-1 Social Discovery Software aggregates social media data in real time. It can capture and instantly search contents from websites, webmail, Facebook, Twitter, and other web posts. The software can be set up to track many "persons of interest" and preserve the data in a way that can be authenticated for admission at trial. One of the many benefits of X1 Social Discovery is its ability to preserve and display all the available "circumstantial indicia" or "additional confirming circumstances," to assist in authenticating social media evidence collected with the software.

Nextpoint social media e-discovery offers enhanced collection of social media data. This tool gives lawyers the ability to collect websites, social media, and blog content and to review it for purposes of litigation. The software automatically collects, preserves, archives, and indexes online content, providing a searchable archive of the data.¹²

§ 20.6 Personal Jurisdiction in the Digital Age

Social media may be relevant also to jurisdictional discovery. Can a tweet or a Facebook post subject a party to jurisdiction in a particular state? The issue of whether a party's activities on social networking platforms like Facebook, Twitter, YouTube,

^{11.} Thanks to Joseph Indelicato, Jr., for permission to use portions of his article *Sex, Drugs and Surveillance*, State Bar of Texas CLE (Apr. 2017).

^{12.} Thanks to Joseph Indelicato, Jr., for permission to use portions of his article Sex, Drugs and Surveillance, State Bar of Texas CLE (Apr. 2017).

Social Media

and LinkedIn can lead to a court finding that it has personal jurisdiction over that party is a still-evolving one around the country, where some courts have answered "yes," while other courts have said "no." In most instances, the nature and extent of the Internet activities in question will be analyzed to determine whether exercising jurisdiction would satisfy due process concerns and be consistent with what the U.S. Supreme Court has characterized as "fair play and substantial justice." Generally speaking, it will usually take more than merely having a Facebook page or Twitter account before a court will find a basis for jurisdiction. However, when those social media accounts are used to target activities or communications to a particular state, it is certainly possible that the account holder may have subjected himself to the court's jurisdiction. This issue has become a greater concern than ever in the age of e-commerce and digital media, in which—as one Texas court has pointed out—the Internet "makes it possible to conduct business throughout the world entirely from a desktop."¹³

How do traditional notions of jurisdiction apply in situations where a customer in one state is, with a few clicks of a mouse, transacting business with a company in another state? The seminal decision on whether minimum contacts exist in a party's operation of an Internet-based business is *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*—a highly influential case that has been cited numerous times.¹⁴ In this case, Zippo Manufacturing filed suit in its home state, Pennsylvania, against a California-based Internet news service, Zippo Dot Com, alleging that it was wrongfully capitalizing on the lighter manufacturer's name and reputation in the marketplace. The trial court held that Pennsylvania could exercise jurisdiction over the California company, pointing out that Zippo Dot Com delivered news to approximately 140,000 subscribers worldwide, of which roughly 3,000 were residents of Pennsylvania.

More importantly, the *Zippo* decision established a sliding scale test to evaluate the "nature and quality of commercial activity that an entity conducts over the Internet." The court's analysis categorized Internet use over a spectrum with three main points. At one end is the purely passive website, where the defendant merely makes information available and there is no interactivity that would enable customers to transact

^{13.} Jones v. Beech Aircraft Corp., 995 S.W.21 767, 772 (Tex. App.—San Antonio 1999), abrogated by BMC Software Belgium, N.V. v. Marchand, 83 S.W.3d 789 (Tex. 2002).

^{14.} Zippo Mfg. Co. v. Zippo Dot Com, Inc, 952 F. Supp. 1119 (W.D. Pa. 1997). But see SprayFoam-Polymers.com, LLC v. Luciano, 584 S.W.3d 44, 53 (Tex. App. 2018), review denied (Mar. 29, 2019), order withdrawn (Oct. 4, 2019), review granted (Oct. 4, 2019), case abated (Feb. 14, 2020) (noting that the United States Supreme Court in Bristol-Myers Squibb Co. v. Superior Court of Cal., 137 S. Ct. 1773, 1781(2017), disapproved of the "sliding scale" approach to specific jurisdiction as originally used in Zippo Manufacturing.

siness. At the opposite end of t

§ 20.6

business. At the opposite end of the spectrum is a highly interactive website, which gives others the ability to, among other things, download, exchange information, and enter into contracts. At the purely passive end of the spectrum, exercising personal jurisdiction over a nonresident defendant is generally improper, while at the highly interactive end of the spectrum—where the activities "involve the knowing and repeated transmission of computer files over the Internet"—jurisdiction over the non-resident defendant is generally proper. The middle point on the spectrum, where information can be exchanged between the person viewing the site and the host computer, presents a thornier question in which the court will have to examine "the level of interactivity and the commercial nature of the exchange of information."¹⁵

The experience of Texas appellate courts in determining whether one's activities on a social networking platform may justify the exercise of jurisdiction is typical of the debate raging in courts nationwide; in other words, it is highly dependent on the facts of each case. In two cases, courts relied at least in part on social media activity by the defendant in order to justify exercising jurisdiction. The 2012 case of Hale v. Richev involved a long-distance feud between the widow and adopted daughter of a deceased country-music singer-songwriter known as George Richey.¹⁶ The facts themselves would make a great country song. After Mr. Richey died, his daughter (California resident Deirdre Hale) allegedly defamed Richey's widow (Texas resident Sheila Richey) by claiming that she'd mishandled Richey's trust fund, neglected his medical needs, and other allegations. Richey filed a defamation lawsuit in Texas and, as a basis for jurisdiction, claimed that Hale (1) committed a tort in Texas, (2) made defamatory comments to a national publication "sold at almost every grocery store in Texas," (3) made defamatory statements to at least one relative in Texas via telephone and text messages, (4) made claims about Richey's administration of a Texas-based trust, and (5) used Facebook as a platform to make defamatory statements to multiple recipients whom Hale knew to be in Texas. The trial court denied Hale's special appearance. In upholding this decision, the Waco court of appeals focused more on what it considered targeted communications such as the calls and text messages to Texas rather than national publications that Texans just happened to read. Nevertheless, the posts on Facebook were among the evidence on which the appellate court relied.

In another Texas case, it was an instance of a business finding out the hard way that social networking is a two-way street: a great platform for promoting one's company

^{15.} Zippo, 952 F. Supp. at 1124.

^{16.} Hale v. Richey, No. 10-11-00187-CV, 2012 WL 89920, at *1 (Tex. App.-Waco Jan. 11, 2012).

Social Media

and attracting new hires, but at the same time a potential portal to jurisdiction.¹⁷ In this case (based on the real life incident that inspired the 2013 movie Captain Phillips starring Tom Hanks), Ruiz and his fellow appellees sued Waterman Steamship Corp. (Waterman) and Maersk Line Ltd. (Maersk) in Texas state court in Houston for negligence under the Jones Act and general maritime law for injuries the crewmen suffered when their vessel, the MV Maersk Alabama, was hijacked by Somali pirates in April 2009. Waterman, an Alabama corporation, and Maersk, a Delaware corporation with its principal place of business in Virginia, objected to the Texas court asserting jurisdiction. The trial court denied their special appearances and the appellate court upheld this denial as to Maersk. In analyzing whether the defendants had sufficient minimum contacts with Texas, the appellate court examined numerous factors, including calls on Texas ports, payment of Texas franchise taxes, and purchases from Texas vendors. But one of the most significant factors in the court's decision to uphold jurisdiction over Maersk (it found Waterman's contact insufficient to confer jurisdiction) was Maersk's reliance on and use of Twitter to solicit business and to advertise in Texas. The court pointed out that when Maersk's ships would dock in Houston's port, they would use their Twitter feed to give estimated times of arrival, "promote the capabilities of its vessels," and "solicit additional cargo for its voyages" when it had unused space.¹⁸ This regular use of Twitter became an important part of what the court considered the "totality of Maersk's contacts with Texas," which the court found was a sufficient basis for jurisdiction.

However, jurisdictional analysis is highly fact-specific, and Texas courts considering online activities have also rejected them as a basis for haling a party into a Texas court. A case from the same appellate district as Ruiz illustrates the point that the mere claim that one has been defamed online—absent facts that show the specific targeting of the forum state—won't be enough to justify jurisdiction. The case of *Wilkerson v. RSL Funding, LLC* involved an individual whose daughter won the California lottery, then sold her rights to future installments in exchange for a lump sum payment from Houston-based RSL Funding, LLC.¹⁹ Wilkerson was less than pleased with her experience, and her father Jerry posted about the company on Yahoo's consumer reviews section and on sites like Yelp. Wilkerson didn't know that both sites would also publish his reviews on "local" pages aimed at Texas residents. RSL Funding sued him for libel and business disparagement in Texas, claiming he had "purposely

^{17.} Waterman Steamship Corp. v. Ruiz, 355 S.W.3d 387 (Tex. App.-Houston [1st Dist.] 2011).

^{18.} Waterman Steamship Corp., 355 S.W.3d 424.

^{19.} Wilkerson v. RSL Funding, L.L.C., 388 S.W.3d 668 (Tex. App.-Houston [1st Dist.] 2011).

directed his actions at Texas," and the trial court agreed, denying his special appearance.

But Houston's First District Court of Appeals disagreed and gave a lengthy and useful analysis in its opinion of how Texas courts have applied the Zippo sliding scale analysis of website interactivity. It adopted a user-centric view that is applicable to individual users of social media. Even though sites like Yelp and Yahoo have a high degree of interactivity under the Zippo test (and so, by extension, do social networking platforms), the use by a third party (like Wilkerson) of such a site could be considered essentially a "passive" usage. The court distinguished between what a site operator like Yelp might have intended in publishing comments on its Texas pages and what Wilkerson individually intended, in terms of whether his activities were expressly aimed at Texas. The court noted that it is "common knowledge" that sites like Yelp and Yahoo "commonly repackage and republish user contributions along with other information like the maps, addresses, photographs, and other identifying characteristics relied upon by RSL."20 The court concluded that since Wilkerson did not intend to direct his comments to a Texas audience and he had no ability to control how Yelp and Yahoo packaged his comments, exercising jurisdiction over this California resident would be inappropriate.²¹

A Texas federal court recently considered the impact that social media activities may have in determining whether or not to exercise jurisdiction. In *Bell v. The Moawad Group, LLC*, plaintiff Keith Bell, a Texas resident and sports psychologist, asserted copyright infringement claims against the Arizona-based Moawad Group, a sports performance consulting firm, and its manager Trevor Moawad. At issue was the alleged infringement of Bell's book *Winning Isn't Normal*, excerpts of which had allegedly been posted by the defendants on Twitter, Instagram, and Facebook. Bell argued that the social media posts could be accessed by Texas residents and that they targeted Texas residents. The court, however, declined to assert jurisdiction over the defendants, finding that the simple fact of posting an allegedly infringing image on their social media accounts that could be accessed in Texas was not sufficient to confer jurisdiction. The court reasoned that plaintiff had not met his burden to show that the posts targeted Texas or were specifically tailored for a Texas audience.²²

^{20.} Wilkerson, 388 S.W.3d at 680 n.12.

^{21.} *Wilkerson*, 388 S.W.3d at 683. In another case, while the court took note of the fact that use of social networking media like YouTube and Twitter were alleged in the case against non-resident political activists, it was their actual visits to Texas that proved to be decisive in ruling in favor of jurisdiction. *Hoagland v. Butcher*, 396 S.W.3d 182 (Tex. App.—Houston [14th Dist.] 2013).

^{22.} Bell v. Moawad Grp., LLC, No. A-17-CA-00073-SS, 2017 WL 2841679, at *1 (W.D. Tex. June 30, 2017).

§ 20.7 Evidentiary Issues

If a picture is worth a thousand words, then a YouTube video that impeaches the opposing party must be priceless. Welcome to the beauty of social media content as evidence: with people posting anything and everything, right down to the minutiae of their daily lives, trial lawyers have a greater resource than ever imagined with which to portray a person in his or her unguarded moments—in contrast to after he or she has been coached and prepared in everything from word choice to body language. But all of the incriminating tweets and Facebook posts will do a party little good if they can't be admitted into evidence.

Certainly, one of the best ways to authenticate social media content is to do so directly; that is, through a direct admission of authorship by the party or witness who created the content. Asking a party to confirm that a particular social networking profile is his or that he uploaded the photos in question or authored the Facebook post is definitely preferable. In a number of states, including Maryland, Connecticut, New York, and Massachusetts, this "direct authentication" is the rule, and courts in these states are distrustful of other means of authentication. In Texas, however (as well as in other states), there is a recognition that due to the highly individualized nature of social networking profiles, sufficient assurance exists that the social media content is indeed what it purports to be, even without direct authentication by the creator of the content. One Texas court even permitted authentication by a witness who reportedly read the statements in question on the defendant's MySpace page—without any personal knowledge that the defendant herself had typed that admission.²³

Tex. R. Evid. 901 allows a party to authenticate evidence by "[a]ppearance, contents, substance, internal patterns, or other cistinctive characteristics, taken in conjunction with circumstances." No Texas case exemplifies the principles of such circumstantial authentication quite like *Tienda v. State* from the Court of Criminal Appeals.²⁴ In *Tienda*, Texas' highest criminal court upheld the murder conviction of Ronnie Tienda, Jr.—a conviction based not on forensic evidence or eyewitness testimony but instead on postings from various MySpace accounts of the defendant. A jury convicted Tienda of murder following an altercation with the victim, David Valadez, at a night-club. On Tienda's MySpace pages (found and testified to by the victim's sister) there was a photo of the appellant with the caption "If you ain't blasting, you ain't lasting" and the notation "Rest in Peace, David Valadez." There was also an embedded link to an audio recording of a song played at the victim's memorial service, statements

^{23.} In re J.W., No. 10-09-00127-CV, 2009 WL 5155784 (Tex. App.-Waco Dec. 30, 2009).

^{24.} Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012).

referring to people "snitching on me" and "it's cool if I get off;" photos of Tienda's tattoos, references to his nickname "Smiley," as well as photos of Tienda's electronic monitoring bracelet and the fact that he was "str8 outta jail and n da club."²⁵ The Dallas court of appeals had been persuaded by all of these (and more) indications of authenticity, observing that "the inherent nature of social networking websites encourages members who choose to use pseudonyms to identify themselves by posting profiles and pictures or descriptions of their physical appearance, personal backgrounds, and lifestyles." This type of individualization, the court went on, "is significant in authenticating a particular profile page as having been created by the person depicted in it. The more particular and individualized the information, the greater the support for a reasonable juror's finding that the person depicted supplied the information." The court of criminal appeals, after similarly describing several dozen messages, photos, and other details, upheld the conviction as well, concluding that "[t]his is ample circumstantial evidence-taken as a whole with all of the individual, particular details considered" that the "MySpace pages belonged to [Tienda] and that he created and maintained them."26

Circumstantial authentication of social media has been followed by subsequent Texas cases. In *Campbell v. State*, an individual convicted of aggravated assault appealed his conviction, claiming that Facebook messages admitting that he should not have put his hands on the victim were wrongly attributed to him.²⁷ The Campbell court acknowledged that there were hurdles to overcome in considering social media evidence:

Facebook presents an authentication concern that is twofold. First, because anyone can publish a fictitious profile under any name, the person viewing the profile has no way of knowing whether the profile is legitimate. . . . Second, because a person may gain access to another person's account by obtaining the user's name and password, the person viewing communications on or from an account profile cannot be certain that the author is in fact the profile owner. Thus, the fact that an electronic communication on its face purports to originate from a certain person's social networking account is generally insufficient standing alone to authenticate that person as the author of the communication.²⁸

^{25.} Tienda, 358 S.W.3d at 644-45.

^{26.} Tienda, 358 S.W.3d at 645.

^{27.} Campbell v. State, 382 S.W.3d 545 (Tex. App.-Austin 2012).

^{28.} Campbell, 382 S.W.3d at 550 (citations omitted).

Social Media

However, the court went on to discuss the multiple Facebook messages alleged to have been sent by Campbell, each of which bore a banner and date stamp at the top with Campbell's name and the date. Not only did Campbell's victim confirm that Campbell had an account and that she received the messages, the court also took note of certain "internal characteristics" that tended to confirm Campbell as the author.²⁹ These included unique speech patterns in the messages that matched Campbell's Jamaican dialect, as well as references to the incident and potential charges (which, at the time, few people would have known about). Taking all of this into consideration along with the victim's testimony that she and Campbell were the only ones with access to the Facebook account (and that, at the time of the incident, she did not have such access), the court held that the Facebook evidence was properly admitted.

Yet another Texas case upheld the use of circumstantial authentication, although the court also noted that there was other, stronger evidence admitted without objection and which supported the same conclusion.³⁰ In *Rene v. State*, the circumstantial authentication of the defendant's MySpace photos included depictions of his gang tattoos, references to his nickname "Lo," and photos of a small boy and girl identified as the defendant's children. The conviction was affirmed.

Other states, including Georgia, Kentucky, Mississippi, Arizona, and California, have embraced circumstantial authentication of social media content, and several have cited *Tienda* in doing so. When it comes to evidentiary issues and social media, it is fair to say that Texas has been on the cutting edge of an already cutting-edge issue.³¹

§ 20.8 Judges and Social Media

Discovery of a judge's social media account may be relevant in determining whether recusal is proper. Can a judge have a presence on social media without violating canons of judicial conduct? Can a jurist be Facebook "friends" with counsel or even parties or does that convey the impression that the "friend" has some sort of special relationship or influence with the judge? The judicial ethics bodies of ten states have examined the issue of judges' social media activities. Florida takes the most restrictive view of all, holding that not only should a judge not have Facebook "friendships" with attorneys, such a connection warrants automatic disqualification of the judge.³²

^{29.} Campbell, 382 S.W.3d at 551.

^{30.} Rene v. State, 376 S.W.3d 302 (Tex. App.-Houston [14th Dist.] 2012).

^{31.} See also Chapter 18 of this book-Authenticity and Admissibility.

^{32.} See, e.g., Domville v. State, 103 So. 3d 184 (Fla. Dist. Ct. App. 2012), disapproved of by Law Offices of Herssein & Herssein, P.A. v. United Servs. Auto. Ass'n, 271 So. 3d 889 (Fla. 2018).

Most states give cautious approval to judges' tentative forays into social networking. And no less an authority than the ABA Standing Committee on Ethics and Professional Responsibility, in its February 2013 ABA Formal Opinion 462 on "Judges' Use of Electronic Social Networking Media," gave a thumbs up—with certain caveats—to the practice. The ABA opinion provides a useful discussion of the benefits of social networking for members of the judiciary while simultaneously sharing some sobering, common sense reminders about social media interaction.

While Texas is not one of the ten states to have formally confronted in an ethics opinion the question of the extent to which a judge may have social media connections, a 2013 Texas appellate opinion does provide a highly useful and instructive discussion of the Texas perspective on judges and social media. Youkers v. State, a criminal appellate case, dealt with a Facebook communication by the victim's father toward the judge.³³ Youkers appealed the revocation of his eight-year prison sentence and community supervision following his conviction on charges of assaulting his pregnant girlfriend. One of the grounds for his appeal was that he allegedly did not receive a fair trial due to the judge's purported lack of impartiality. The judge in question was Facebook friends with the girlfriend's father, and had received an ex parte communication from this friend.³⁴ At the hearing on Youkers's motion for new trial, the judge testified that he knew the girlfriend's father as a result of them both having run for office during the same election cycle and that although they were friends on Facebook, that was the extent of their relationship. Their only Facebook communication took place just prior to Youkers's original plea, when the father sent a Facebook message to the judge seeking leniency for the defendant. The trial judge responded online formally, advising the father that his communication violated the rules; that any further communication about the case, or any other pending legal matter, would result in "de-friending"; and that the judge was placing a copy of the communication in the court's file, disclosing it to the lawyers and contacting the judicial conduct commission. The father responded with an apology and a promise not to make comments relating to criminal cases in the future.

In a thorough and well-reasoned opinion, Justice Mary Murphy of the Dallas Fifth District Court of Appeals pointed out that this was a case of first impression in Texas, since "no Texas court appears to have addressed the propriety of a judge's use of social media websites such as Facebook. Nor is there a rule, canon of ethics, or judicial ethics opinion in Texas proscribing such use."³⁵ Justice Murphy went on to cite

^{33.} Youkers v. State, 400 S.W.3d 200 (Tex. App.-Dallas 2013).

^{34.} Youkers, 400 S.W.3d at 204.

Social Media

ABA Judicial Ethics Opinion 462 approvingly, both for the beneficial aspects of allowing judges to use social media (i.e., remaining active in the community) and for the concept that the status of being Facebook friends is not necessarily representative of "the degree or intensity of a judge's relationship with that person."³⁶ As the court pointed out, "the designation, standing alone, provides no insight into the nature of the relationship."³⁷ Furthermore, in examining the record for further context, the court noted that there was nothing to indicate that the "Facebook friendship" between the judge and the girlfriend's father—who was actually asking for leniency—was any-thing but a fleeting acquaintance.³⁸

Even more importantly, the court observed, the trial judge had fully complied with the state protocol for dealing with ex parte communications. And while the appellate court noted that judges should, in using social media, remain mindful of their responsibilities under applicable judicial codes of conduct, everything about this judge's actions was consistent with promoting public confidence in the integrity and impartiality of the judiciary. Significantly, the court concluded that while new technology may have ushered in new ways to communicate and share information, the same ethics rules apply: "[W]hile the internet and social media websites create new venues for communication, our analysis should not change because an ex parte communication occurs online or offline."³⁹

§ 20.9 Juries and Social Media

One of the unfortunate byproducts of the digital age is the rise in incidents of online misconduct by jurors, often resulting in mistrials and overturned verdicts. Counsel may consider the ongoing monitoring of jurors' "social media" in both the voir dire phase and throughout the trial.

The problem of the "Googling juror" has been well-documented in recent years, and both state and federal courts all over the country have attempted to address it.⁴⁰ Texas has not been spared in what some legal observers have characterized as an epidemic. In the 2006 case of *Sharpless v. Sims*, after a jury in a double-fatality motor vehicle

- 36. Youkers, 400 S.W.3d at 205-06.
- 37. Youkers, 400 S.W.3d at 206.
- 38. Youkers, 400 S.W.3d at 206.
- 39. Youkers, 400 S.W.3d at 206.
- 40. See John G. Browning, The Online Juror, 93 Judicature 6 (May/June 2010).

^{35.} Youkers, 400 S.W.3d at 205.

accident returned a verdict in favor of the victims' family, the parties learned that one of the jurors had conducted her own independent Internet research. The juror had found the defendant truck driver Sharpless's driving record (which, like evidence of his drug use, had been excluded from evidence). Lawyers for Sharpless and his employer sought a new trial on grounds of jury misconduct, but the Dallas court of appeals ultimately denied their efforts, pointing out that the research wouldn't have led to a different result (the "Googling juror" in question had in fact been in the minority finding for the trucker). And more recently, in 2012 a Tarrant County juror in a car wreck case found himself in trouble when he sent a Facebook friend request to the attractive young female defendant—during trial. As a result, the would-be online Romeo was dismissed from the jury, found in contempt of court, and sentenced to two weeks of community service.

As concerns of Googling jurors mounted, Texas did what many states did—it revised its instructions and admonishments to jurors and prospective jurors to address the problem of jurors venturing online to research the issues or parties or to communicate with third parties about the case while serving on the jury. Effective April 1, 2011, the Supreme Court of Texas amended Texas Rule of Civil Procedure 284 as well as the jury instructions prescribed by rule 226a. Under rule 284, judges must instruct jurors immediately after they are selected for a case "to turn off their cell phones and other electronic devices and not to communicate with anyone through any electronic device while they are in the courtroom or while they are deliberating." In addition, the court must also instruct them that "while they are serving as jurors, they must not post any information about the case on the Internet or search for any information outside of the courtroom, including on the Internet, to try to learn more about the case."

In addition, the instructions to prospective jurors include admonishments to not communicate with anyone through any electronic device, and to "not communicate by phone, text message, e-mail message, chat room, blog, or social networking websites such as Facebook, Twitter, or MySpace." Similarly, jurors are also reminded in the formal instruction and in the court's charge as follows:

Do not discuss the case with anyone else, either in person or by any other means. Do not do any independent investigation about the case or conduct any research. Do not look up any words in dictionaries or on the Internet. Do not post information about the case on the Internet. Do not share any special knowledge or experiences with the other jurors. Do not use your cell phone or any other electronic device during your deliberations for any reason.⁴¹

In an age in which digital intimacy has become the new normal and where the sanctity of a jury room can be violated at the speed of a search engine, measures like these have become an unfortunate necessity in Texas and everywhere else.

§ 20.10 Criminal Law

Social media continues to play a role in shaping Texas criminal law, and not just in terms of the admissibility of evidence. For example, in one recent case, the complainant in an armed robbery case saw the two men who robbed him and asked someone with them for their names. He then looked them up on Facebook, finding (among other things) a photo of one defendant posing with guns—including one identical to a gun stolen from the victim during the robbery.⁴² The crime victim then e-mailed the Facebook photos to the investigating detective and later identified both robbers in separate photo lineups. When the defendant appealed his conviction, claiming that the photo array was impermissibly suggestive, the court rejected the argument, noting that technology was having an impact when it came to shoring up the sometimes questionable reliability of eyewitness testimony. As the court observed, "[v]ast online photo databases—like Facebook—and relatively easy access to them will undoubt-edly play an ever-increasing role in identifying and prosecuting suspects."⁴³

Social media has played a role in other aspects of the criminal justice system, including revocation of probation. It is even mentioned in a case involving alleged Brady violations by the prosecution involving their voluntary dismissal of a state's witness with whom the state had been communicating via Facebook.⁴⁴ In another case, a prisoner complained that rights were being violated when he was "randomly" drug tested after guards became aware of certain content on his Facebook page.⁴⁵ The court held that there was nothing wrong with corrections officials monitoring the social media activities of inmates, not only because "[p]risoners do not have the same expectation of privacy enjoyed by citizens in the free world," but also because such monitoring "is not an unreasonable measure given . . . the intractable problem of controlled substances in the prisons."⁴⁶

41. Browning, The Online Juror.

42. Bradley v. State, 359 S.W.3d 912 (Tex. App.-Houston [14th Dist.] 2012).

43. Bradley, 359 S.W.3d at 918.

44. Fitch v. State, No. 10-11-00283-CR, 2013 WL3770952 (Tex. App.-Waco, July 18, 2013, no pet.).

45. McNickles v. Amaral, No. CIV.A. H-12-3692, 2013 WL 2295407 (S.D. Tex. May 23, 2013).

46. McNickles, 2013 WL 2295407, at *4.

It is in the area of criminal law that we've seen perhaps the most frequent use of, as well as challenges to, social media content as evidence. For example, in *Gonzalez v. State*, the Texas Court of Criminal Appeals weighed the effect of admitting evidence of Facebook messages regarding the defendant's use of ecstasy six to seven hours before his capital murder of a police officer.⁴⁷ The appellant argued that such evidence was not relevant, that it was improper character evidence, and that its prejudicial nature outweighed its probative value. The Court agreed that, under rule 403, the evidence of guilt and the prosecution's lack of emphasis of these particular messages. And in reality, there were other Facebook messages that were far more problematic for Gonzales, including one that he sent to a friend the evening of the incident that read "I hope you didn't get caught. I killed the guy. He went into compulsions [sic] and died."

As the popularity of particular social networking platforms rises, a corresponding rise in the use of evidence from those cites occurs as well. The MySpace profile so instrumental in the *Tienda* case, for example, has been overtaken by evidence from platforms like Instagram. See, for example, *Mohamed v. State*, Case No. 05-15-01329-CR (Tex. App.—Dallas, Dec. 6, 2016) (Instagram evidence properly admitted); *Jones v. State*, Case No. 01-18-00154-CR (Tex. App.—Houston [1st Dist.] July 11, 2019) (Instagram evidence properly admitted); and *United States v. Ballesteros*, 751 F. App'x 579 (5th Cir. 2019) (Facebook profile's admission did not violate the hearsay rule).

Courts in Texas have made relatively short work of challenges to the admissibility of a party's own statements on Facebook. For example, in *Bullman v. State*, the Beaumont court of appeals included a comprehensive discussion of authentication of social media evidence from *Tienda* forward before rejecting Bullman's challenge to the admission of his own Facebook statements.⁴⁸ The Court held that, per Texas Rule of Evidence 801(e)(2)(A), a defendant's own statements, when offered against him, are not hearsay; accordingly, because the Facebook messages in question were posted by Bullman himself, the trial court had properly overruled his hearsay objections.

However, it is a different story when attempts are made to introduce the Facebook posts made by third parties. That was the issue in *Dering v. State*, in which Dering (convicted of aggravated sexual assault of an elderly person) challenged the trial court's failure to admit Facebook posts made by third parties, which Dering sought to

^{47.} Gonzalez v. State, 544 S.W.3d 363, 368 (Tex. Crim. App. 2018).

^{48.} Bullman v. State, No. 09-14-00196-CR, 2016 WL 1469592, at *1 (Tex. App.—Beaumont Apr. 13, 2016).

Social Media

introduce in support of a motion to transfer venue.⁴⁹ Dering did not call any of the thirty-one authors of these posts to authenticate the statements, nor did he make any other effort at authentication. On appeal, the Eastland court of appeals provided a comprehensive discussion of Texas Rule of Evidence 901 and authentication of social media evidence, including *Tienda* and its progeny. It also acknowledged the different nature of the situation before the court, in which the evidentiary issue involved commentary on a social media cite by third parties rather than posts made by or sent to the appellant himself. Noting that the posts were created by third parties who did not testify during the proceedings, and that there "was no evidence of the authenticity of who the purported author was of any of the Facebook posts," the Court held that there was insufficient evidence to support a finding of authenticity. Moreover, the Court held that any error would have been harmless since exposure to media, including social media, had little to no effect on the jury pool as a whole.

Social media can play a pivotal role in the modern criminal trial, as high-profile cases like the George Zimmerman case in Florida have demonstrated. Content from social networking sites has been used in Texas criminal cases for everything from proving gang affiliation⁵⁰ to establishing state of mind.⁵¹ Use of such content will only assume a more prominent role as time goes on.

§ 20.11 Conclusion

Discovery of relevant social media is oftentimes crucial in establishing liability in a civil case or guilt or innocence in a criminal case. Nevertheless, courts are cognizant of intrusion into private and nonrelevant matters. Holders of relevant social media have a duty to preserve such evidence once the duty to preserve has been triggered. When obtaining relevant social media, a party should be cognizant of establishing the evidentiary framework that will allow for the introduction of that social media into evidence.

^{49.} Dering v. State, 465 S.W.3d 668, 672 (Tex. App.-Eastland 2015).

^{50.} *Munoz v. State*, No. 13-08-00239-CR, 2009 WL 695462 (Tex. App.—Corpus Christi–Edinburg Jan. 15, 2009).

^{51.} Hall v. State, 283 S.W.3d 137 (Tex. App.-Austin 2009).



Chapter 21

Discovery of ESI from Nonparties

Stephen Orsinger

§ 21.1 Introduction

This chapter addresses the standards and procedures for acquiring discovery of electronically stored information ("ESI") from nonparties in both state and federal courts in Texas. The law has not developed many rules for nonparty discovery unique to ESI, though there are some special rules applicable to the discovery of ESI from parties that could also impact nonparties. As a result, this chapter describes the state and federal framework for nonparty discovery in general and focuses on special issues involving ESI when they arise.

§ 21.2 Texas Standards and Procedures

There are four primary mechanisms for obtaining particular types of discovery from nonparties: (1) subpoenas under Texas Rule of Civil Procedure 205, (2) court orders permitting presuit depositions under Texas Rule of Civil Procedure 202, (3) court orders requiring a physical or mental examination under Texas Rule of Civil Procedure 204, and (4) court orders permitting entry on property for examination under Texas Rule of Civil Procedure 196.7.

In theory, ESI may be sought or generated with all four of these mechanisms, but it usually only arises in the context of the first and second. This pair comprises the vast majority of nonparty discovery attorneys encounter and is the primary focus of this chapter.

§ 21.2:1 Rule 205—Subpoena

The Texas Rules of Civil Procedure specifically govern discovery from nonparties.¹ These rules establish the procedure for obtaining nonparty discovery by means of a subpoena compelling one of four types of discovery. They are—

^{1.} See Tex. R. Civ. P. 205.1, 205.2, 205.3.

- 1. oral depositions;
- 2. depositions on written questions;
- 3. requests for production accompanied by a deposition notice; and
- 4. requests for production unaccompanied by a deposition notice.²

However, ESI itself is not obtained in a deposition, but instead only through a request for production of that ESI.

§ 21.2:2 Issuing Subpoena

The subpoena is an integral component of acquiring ESI from a nonparty. The subpoena may be issued by the court's clerk, an attorney licensed in Texas, or an officer of the court authorized to take depositions after receiving a rule 205 notice to take a deposition.³

§ 21.2:3 Requests for Production with Deposition Notice

A party may secure ESI from a nonparty through the deposition procedure. The subpoena for the production of documents or tangible things (referred to commonly as a "subpoena duces tecum") may be served on a nonparty along with a notice of deposition on oral examination or written questions.⁴ The procedures for noticing either type of deposition on a nonparty are the same as they are for parties generally.⁵

For an oral deposition, the list of ESI to be produced must be included in the subpoena, as well as either attached to or included in the deposition notice.⁶ The notice must be served on the nonparty either before or simultaneously with service of the subpoena compelling attendance and production⁷ and must be served a reasonable time before the deposition is to be taken.⁸

- 2. Tex. R. Civ. P. 205.1.
- 3. Tex. R. Civ. P. 176.4.
- 4. Tex. R. Civ. P. 205.1(c).
- 5. Tex. R. Civ. P. 199.2, 200.1, 205.1(c).
- 6. Tex. R. Civ. P. 199.2(b)(5).
- 7. Tex. R. Civ. P. 205.2.
- 8. Tex. R. Civ. P. 199.2(a).
What constitutes a "reasonable time" for service of notice of an oral or written deposition is case specific.⁹ Most cases interpreting reasonable notice focus on time periods within ten days, with less than five days' notice usually (but not always) assessed as unreasonable and more than five days' notice usually assessed as reasonable.¹⁰

A written deposition follows many of the same rules applicable to oral depositions.¹¹ The list of ESI to be produced must be included in the subpoena, as well as either attached to or included in the deposition notice.¹² Again, the notice for a written deposition must be served on the nonparty either before or simultaneously with service of the subpoena compelling production,¹⁵ but unlike oral depositions the notice must be served on the deponent and all parties at least twenty days before the deposition is to occur.¹⁴

The general rule for the other contents of the notice is the same for both types of depositions.¹⁵ The conducting of a written deposition follows a similar procedure for the conducting of an oral deposition.¹⁶

§ 21.2:4 Requests for Production without Deposition Notice

A party may also request ESI from a nonparty without taking a deposition.¹⁷ As with production pursuant to a deposition, this type of request requires both a subpoena and notice.¹⁸ The notice must be served at least ten days before the subpoena compelling

13. Tex. R. Civ. P. 205.2.

16. Cf. Tex. R. Civ. P. 200.3, 200.4, 199.5.

17. One important function of a nonparty deposition—whether in person or on written questions is to provide a convenient means by which the documents produced by the deponent can be authentcated. While ESI produced by a nonparty can still be authenticated in other ways (such as by a business records affidavit or live testimony) it is advisable to authenticate the nonparty discovery at the time it is initially produced through the deposition process.

18. Tex. R. Civ. P. 205.3(a).

^{9.} *Hycarbex, Inc. v. Anglo-Suisse, Inc.*, 927 S.W.2d 103, 111 (Tex. App.—Houston [14th Dist.] 1996, no writ) (interpreting predecessor to rule 199).

^{10.} See Hycarbex, 927 S.W.2d at 111–12 (four days' notice unreasonable); Hogan v. Beckel, 783 S.W.2d 307, 309 (Tex. App.—San Antonio 1989, writ denied) (same); Bohmfalk v. Linwood, 742 S.W.2d 518, 520 (Tex. App.—Dallas 1987, no writ) (four days' notice reasonable); Gutierrez v. Walsh, 748 S.W.2d 27, 28 (Tex. App.—Corpus Christi–Edinburg 1988, no writ) (six and eight days' notice reasonable).

^{11.} See Tex. R. Civ. P. 200.1(b).

^{12.} Tex. R. Civ. P. 200.1(b), 199.2(b)(5).

^{14.} Tex. R. Civ. P. 200.1(a).

^{15.} Tex. R. Civ. P. 199.2(b), 200.1(b).

production,¹⁹ and that notice must also be served a reasonable time before the deposition is to be taken.²⁰

The content of the notice is governed by a special rule that tracks the general requirements of requests for production made in connection with depositions.²¹ Such requirements include identification of the ESI to be produced and the time and place of production.²²

§ 21.3 Cost of Production

The rules for the costs of production of ESI from a nonparty differ from the cost-shifting analysis applicable to the production of ESI from a party.

The long-standing general rule is that a person responding to a discovery request bears the costs of production.²³ Under the cost-shifting analysis for production of ESI *from parties*, the requesting party is only required to pay the reasonable expenses of any extraordinary measures required to produce the ESI.²⁴

The rule *for nonparties* is at the opposite end of the spectrum: the requesting party must reimburse all of the nonparty's reasonable costs of production.²⁵ Furthermore, the party issuing the subpoena to the nonparty must also take reasonable steps to avoid imposing undue burden or expense on that nonparty.²⁶ This rule significantly differs from federal rule 45, which applies the federal cost-shifting analysis to nonparties, as well.

§ 21.4 Specificity of Notice

Separate requirements for notices requesting production of ESI have developed through the case law. While these requirements have only been applied in the context of a party's production of ESI pursuant to a standard rule 196.4 request, rule

- 21. Cf. Tex. R. Civ. P. 205.3(b), 199.2(b).
- 22. Tex. R. Civ. P. 205.3(b).

23. See Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 428–29 (S.D.N.Y. 2002).

- 24. Tex. R. Civ. P. 196.4.
- 25. Tex. R. Civ. P. 205.3(f).
- 26. Tex. R. Civ. P. 176.7.

^{19.} Tex. R. Civ. P. 205.2.

^{20.} Tex. R. Civ. P. 205.3(a).

199.2(b)(5) invokes both rule 196 and rule 205. Rule 205.3 requires the identification of the material to be produced "with reasonable particularity," while rule 196.4 requires a party to "specifically request production" of ESI.²⁷

Even though the rule 196.4 specificity requirement is not directed toward nonparty discovery, the reasons underlying the requirement-to ensure that requests for ESI are clearly understood and disputes avoided-would seem to apply equally to both parties and nonparties.²⁸ For those same reasons, the following analysis of the specificity of the notice requesting production of ESI from parties could also be applied to notice to nonparties.

Both Texas²⁹ and the federal courts³⁰ recognize that a requesting party should specifically request production of electronic information.³¹ However, at the outset of litigation, the requesting party might not yet know enough about the responding party's computer system, retention procedures, or means of creating and storing information to fashion a sufficiently specific request.

In *Weekley Homes*, the requesting party did not specifically request the production of "deleted e-mails" and could have made such a request without needing an intricate knowledge of the responding party's computer system.³² Nevertheless, the court determined that the responding party "understood" that deleted e-mails were being requested and therefore "was not prejudiced by" the lack of specificity in the request.³³ Thus, there was no abuse of discretion in ordering their production, despite rule 196.4.³⁴

The court also limited the specificity requirement by stating that "knowledge as to the particular *method or means of retrieving* [ESI] is not necessary at the requesting state of discovery."³⁵ However, the court strongly encouraged the requesting party to com-

31. Notice, however, that specificity is an explicit requirement under the Texas Rules of Civil Procedure, but merely a factor to be considered in the cost-shifting analysis on the federal level.

32. Weekley Homes, 295 S.W.3d at 314.

33. Weekley Homes, 295 S.W.3d at 314–15.

34. Weekley Homes, 295 S.W.3d at 315.

35. Weekley Homes, 295 S.W.3d at 314 (emphasis added).

^{27.} Tex. R. Civ. P. 205.3(b)(3), 196.4.

^{28.} See In re Weekley Homes, L.P., 295 S.W.3d 309, 314-15 (Tex. 2009) (orig. proceeding).

^{29.} Tex. R. Civ. P. 196.4 ("[T]he requesting party must *specifically request* production of electronic or magnetic data." (emphasis added)).

^{30.} Rowe, 205 F.R.D. at 429; Zubulake v. JBS Warburg LLC, 217 F.R.D. 309, 321 (S.D.N.Y. 2003).

municate with the responding party regarding the latter's electronic storage systems and procedures, as well as potential methods of retrieval of ESI.³⁶

In sum, the specificity requirement is only violated if the responding party is prejudiced by the lack of specificity. However, requesting parties should always make their discovery requests as clear as possible with the knowledge they have. They need not understand the particularities of the responding party's computing system prior to making their request, but should communicate with them after the request is made to determine the feasibility of production of the ESI.

§ 21.5 Rule 202—Presuit Depositions

Presuit depositions are used as a means of investigating a potential claim or suit or securing testimony for an anticipated suit.³⁷ Because no suit is actually pending, any such discovery is technically from a nonparty.³⁸

§ 21.5:1 Petition to Take Deposition

The person wishing to take a presuit deposition must petition a court for permission to do so. The various requirements of this petition are outside the scope of this chapter but generally include an explanation of the potential or anticipated suit, as well as an identification of the potential parties and deponent, the substance of the testimony to be elicited, and the reasons for requesting that testimony.³⁹ The petition must be verified.⁴⁰

§ 21.5:2 Notice of Hearing on Petition

Notice of the hearing on the petition for presuit discovery must be made on the deponent and the potential or anticipated party at least fifteen days before the date of the hearing. This time period may be modified by the court, as justice or necessity require.⁴¹

36. Weekley Homes, 295 S.W.3d at 314, 315 n.6.

- 37. Tex. R. Civ. P. 202.1.
- 38. See Tex. R. Civ. P. 202.5.
- 39. Tex. R. Civ. P. 202.2.
- 40. Tex. R. Civ. P. 202.2.
- 41. Tex. R. Civ. P. 202.3(d).

The notice must be served under rule 21a, the standard rule for service applicable to most filings.⁴² Special provisions for service by publication are employed for presuit discovery, however.⁴³

§ 21.5:3 Notice of Deposition

The court's order permitting the presuit deposition must prescribe the method of the deposition and may set its time and date.⁴⁴ If the order does not set the time and date for the deposition, the person authorized to conduct the presuit discovery may notice the deposition himself under either rule 199 or 200.⁴⁵ The notice procedures established by those rules are described at length above and are applicable to the presuit deposition notice.

§ 21.5:4 Applicability of Rules for Nonparty Discovery

A presuit deposition is "governed by the rules applicable to depositions of nonparties in a pending suit."⁴⁶ As a result, the form of the presuit deposition notice, its contents, and the timing of its service all follow the rules described above. Rule 202 does not contain any specific subpoena requirement, and the court order authorizing the deposition would seem to serve the same function. However, there would be little harm in reading rule 202.5 strictly and issuing a subpoena along with or after (as applicable) the rule 202.4 notice.

§ 21.6 Rule 204—Mental Examinations

Though the discovery mechanism of mental examinations does not often directly involve ESI, the examination itself may incorporate testing that generates ESI. Computer-assisted psychological assessment and computer-based test interpretation programs incorporate data and functions that are not usually apparent from the output of the program. These hidden data and functions are conceptually (and definitionally) metadata, which is generally discoverable.⁴⁷

- 43. Cf. Tex. R. Civ. P. 202.3(b), 109.
- 44. Tex. R. Civ. P. 202.4(b).
- 45. Tex. R. Civ. P. 202.4(b).
- 46. Tex. R. Civ. P. 202.5.
- 47. See In re Honza, 242 S.W.3d 578, 581 (Tex. App.-Waco 2008, orig. proceeding).

^{42.} Tex. R. Civ. P. 202.3(a), 21a.

Because the court's order must specify the manner, conditions, and scope of the mental examination of a nonparty,⁴⁸ if ESI will be generated during the mental examination, the party requesting this discovery mechanism should ensure that provisions for the production of that ESI be included in that order. The nonparty may also access this ESI by means of a request under rule 204.2 for the examiner to report its findings, "including results of all tests made."⁴⁹

§ 21.7 Rule 196.7—Entry on Property for Examination

As with the mental examination, this discovery mechanism does not often directly involve ESI. However, rule 196.7 permits entry onto property in order to "measure, survey, photograph, test, or sample the property."⁵⁰ Any of these five actions may involve the creation of ESI.

The court's order must state the manner, conditions, and scope of the inspection and must specifically describe any desired means, manner, and procedure for testing or sampling.⁵¹ Therefore, the party requesting this discovery mechanism should ensure that provisions for the production of any ESI that is created be included in that order.

§ 21.8 Federal Standards and Procedures

Under the Federal Rules of Civil Procedure, a nonparty may be compelled to produce ESI or permit entry onto property for examination.⁵² Both types of nonparty discovery are governed by rule 45. This rule underwent significant revision effective December 1, 2013; the new version is described in this section, with occasional reference to its predecessor.

§ 21.9 Rule 45—Subpoena

Unlike the Texas Rules of Civil Procedure, the Federal Rules of Civil Procedure specifically incorporate provisions pertinent to ESI into their subpoena rule. Rule 45 governs the issuance of all subpoena, including those to nonparties.

- 48. Tex. R. Civ. P. 204.1.
- 49. Tex. R. Civ. P. 204.2(a).
- 50. Tex. R. Civ. P. 196.7(a).
- 51. Tex. R. Civ. P. 196.7(b).
- 52. Fed. R. Civ. P. 34(c).

"Federal Rule of Civil Procedure 45 'explicitly contemplates the use of subpoenas in relation to nonparties' and governs subpoenas served on a third party . . . as well as motions to quash or modify or to compel compliance with such a subpoena."⁵³

Rule 45 provides certain specific rules as to the form of production of ESI,⁵⁴ but otherwise, as with the federal rules governing discovery from a party, the federal rules do not provide special rules for requests for ESI from nonparties.

§ 21.9:1 Form and Contents

As with its Texas counterpart, rule 45 permits a discovery subpoena to issue along with or independently from a subpoena commanding attendance at a deposition.⁵⁵ The subpoena must specify the time and place at which the producing party must produce ESI and testify, if applicable.⁵⁶ If the subpoena requests ESI, it "may specify the form or forms in which electronically stored information is to be produced."⁵⁷

§ 21.9:2 Issuance, Enforcement, and Protection

One of the important changes made to rule 45 is the location of the court issuing the subpoena. Under the old version of the rule, the court that issued the subpoena was the court with territorial jurisdiction over the nonparty from whom discovery was sought, and the subpoena had to comply with the rules of form for that foreign court. In situations in which subpoenas for multiple nonparties in diverse jurisdictions were being issued, the requesting party could face a significant burden in drafting several different subpoenas for each of these nonparties.

The new rule eliminates this potential problem by designating the court in which the suit is pending as the "issuing court."⁵⁸ Enforcement of or protection from these subpoenas is ordered by the court for the district in which compliance is required—the "enforcement court"—under both old and new versions of the rule.⁵⁹

- 56. Fed. R. Civ. P. 45(a)(1)(A)(iii).
- 57. Fed. R. Civ. P. 45(a)(1)(C).
- 58. Fed. R. Civ. P. 45(a)(2).
- 59. Fed. R. Civ. P. 45(d).

^{53.} Am. Fed'n of Musicians of the U.S. & Canada v. SKODAM Films, LLC, 313 F.R.D. 39, 42 (N.D. Tex. 2015) (quoting Isenberg v. Chase Bank USA, N.A., 661 F. Supp. 2d 627, 629 (N.D. Tex. 2009)).

^{54.} See Fed. R. Civ. P. 45(a)(1)(C), (e)(1).

^{55.} Fed. R. Civ. P. 45(a)(1)(C).

Once properly served with a rule 45 subpoena, a nonparty is subject to discovery obligations that the subpoena imposes, within the rule 45 protections that the nonparty is entitled to invoke.⁶⁰ To invoke those protections through objections, rule 45(d)(2) requires that the subpoenaed party "serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored

Under Federal Rule of Civil Procedure 45(d)(1), "[a] party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena," and "[t]he court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply."⁶²

Federal Rule of Civil Procedure 45(d)(2)(B) requires that "[a] person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested"—and that "[t]he objection must be served before the earlier of the time specified for compliance or fourteen days after the subpoena is served."⁶³

Under rule 45(d)(2)(B)—

information in the form or forms requested."61

[i]f an objection is made, the following rules apply: (i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection. (ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.⁶⁴

64. Fed. R. Civ. P. 45(d)(2)(B).

^{60.} See Andra Group, LP v. JDA Software Group, Inc., No. 3:15-mc-11-K-BN, 2015 WL 1636602, at *6 (N.D. Tex. Apr. 13, 2015).

^{61.} Fed. R. Civ. P. 45(d)(2)(B).

^{62.} Fed. R. Civ. P. 45(d)(1); see also Am. Fed'n of Musicians of the U.S., 313 F.R.D. at 57-59.

^{63.} Fed. R. Civ. P. 45(d)(2)(B).

Discovery of ESI from Nonparties

Timely serving written objections therefore suspends the nonparty's obligation to comply with a subpoena commanding production of documents, pending a court order.⁶⁵ And rule 37(a) generally does not apply to motions to enforce a subpoena against a third party—rather rule 45(d)(2)(B)(i) governs a party's motion to compel a third party to comply with a rule 45(a) subpoena.

Courts have also held that "a nonparty's rule 45(d)(2)(B) objections to discovery requests in a subpoena are subject to the same prohibition on general or boilerplate [or unsupported] objections and requirements that the objections must be made with specificity and that the responding party must explain and support its objections."⁶⁶ According to this interpretation of the rules, just as, "[a]lthough [Federal Rule of Civil Procedure] 34 governs document discovery from a party and not a nonparty, see Fed. R. Civ. P. 34(c)," "rule 34(b)(1)'s reasonable particularity requirement should apply with no less force to a subpoena's document requests to a nonparty," so too "a nonparty's rule 45(d)(2)(B) objections to those requests should be subject to the same requirements facing a party objecting to discovery under rule 34."⁶⁷

This means that a nonparty is subject to the requirements that an objection to a document request must, for each item or category, state with specificity the grounds for objecting to the request, including the reasons, and must state whether any responsive materials are being withheld on the basis of that objection; that an objection to part of a request must specify the part and permit inspection of the rest; that "general or socalled boilerplate or unsupported objections are improper under rule 45(d)(2)(B)"; and the requirements to make proper objections and how to properly respond to discovery requests apply equally to nonparties subject to a rule 45 subpoena.⁶⁸

Under Federal Rule of Civil Procedure 45(d), "[e]ither in lieu of or in addition to serving objections on the party seeking discovery, a person can 'timely' file a motion to quash or modify the subpoena" under Federal Rule of Civil Procedure 45(d)(3)(A).⁶⁹ Under Rule 45(d)(3)(A)—

69. In re Ex Parte Application of Grupo Mexico SAB de CV, No. 3:14-mc-73-G, 2015 WL 12916415, at *3 (N.D. Tex. Mar. 10, 2015), aff'd sub nom. Grupo Mexico SAB de CV v. SAS Asset Recovery, Ltd., 821 F.3d 573 (5th Cir. 2016).

^{65.} See Fed. R. Civ. P. 45(d)(2)(B)(ii); Am. Fed'n of Musicians of the U.S., 313 F.R.D. at 44.

^{66.} Am. Fed'n of Musicians of the U.S., 313 F.R.D. at 46 (citing Heller v. City of Dallas, 303 F.R.D. 466, 483 (N.D. Tex. 2004), and adopting "the explanations in Heller of what is required to make proper objections and how to properly respond to discovery requests").

^{67.} Am. Fed'n of Musicians of the U.S., 313 F.R.D. at 43, 46.

^{68.} See Am. Fed'n of Musicians of the U.S., 313 F.R.D. at 46; Fed. R. Civ. P. 45(d)(2)(B)-(C).

[o]n timely motion, the court for the district where compliance is required must quash or modify a subpoena that (i) fails to allow a reasonable time to comply; (ii) requires a person to comply beyond the geographical limits

specified in Rule 45(c); (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or (iv) subjects a person to undue burden.⁷⁰

And, "[i]n the majority of cases, a person—whether a traditional party (i.e., a plaintiff or defendant) or a nonparty—waives objections if he/she/it fails either to serve timely objections on the party seeking discovery or to file a timely motion with the court."⁷¹

As one judge in the Fifth Circuit has explained:

When a nonparty to a lawsuit . . . is served with an overly broad subpoena duces tecum, . . . the nonparty has four procedural options. First, it may ignore the subpoena. This is the worst option, almost certain to result in a contempt citation under rule 45(g) and a finding that all objections have been waived. Second, the nonparty may comply with the subpoena, an option that appears to be less frequently chosen in these contentious times.

Third, the nonparty "*may* serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested." Fed. R. Civ. P. 45(d)(2)(B) (emphasis added). Significantly, this rule uses the permissive "may." It does not use the mandatory "shall" or "must." The non-party is not required to serve written objections. Instead, serving written objections is a less formal, easier, usually less expensive method of forestalling subpoena compliance when compared to the separate option of filing a motion to quash or modify the subpoena, as discussed below. However, if the subpoena recipient chooses to serve written objections rather than file a motion to quash or modify, the objections must be served on the issuing party "before the earlier of the time specified for compliance or fourteen days after the subpoena is served."

^{....}

^{70.} Fed. R. Civ. P. 45(d)(3)(A).

^{71.} Grupo Mexico, 2015 WL 12916415, at *3; accord Am. Fed'n of Musicians of the U.S., 313 F.R.D. at 43 (explaining that "[t]he failure to serve written objections to a subpoena within the time specified by rule [45(d)(2)(B)] typically constitutes a waiver of such objections, as does failing to file a timely motion to quash." (internal quotation marks omitted)).

Serving written objections under rule 45(d)(2)(B) may provide the recipient with several advantages. For example, asserting objections can be done informally without going to court, shifts the burden and expense of commencing motion practice in court to the issuing party and affords the recipient additional time in the event the recipient is ultimately obligated to comply with the demands in the subpoena.

The nonparty's fourth option is the one that [the non-party] elected to exercise in this case. Under rule 45(d)(3), the subpoena recipient may move to modify or quash the subpoena as a means of asserting its objections to the subpoena. Unlike serving rule 45(d)(2)(B) written objections, a motion to quash is not subject to the fourteen-day requirement. Instead, the rule provides simply that the motion to quash must be "timely." Fed. R. Civ. P. 45(d)(3)(A). As the leading commentators and the case law they rely upon explain, the "fourteen-day requirement to object to a subpoena is not relevant to a motion to quash a subpoena . . ." Wright & Miller (emphasis added) and cases cited at n.10, including COA Inc. v. Xiamei Houseware Group Co., Inc., No. C13-771 MJP, 2013 WL 2332347, *2 (W.D. Wash. May 28, 2013) (quoting King v. Fidelity Nat. Bank of Baton Rouge, 712 F.2d 188, 191 (5th Cir. 1983)); In re Kulzer, No. 3:09-MC-08 CAN, 2009 WL 961229 (N.D. Ind. Apr. 8, 2009), rev'd on other grounds Heraeus Kulzer, GmbH v. Biomet, Inc., 633 F.3d 591 (7th Cir. 2011) (motion to quash was timely even though it was not served within 14-day time limit).

. . . .

Rules 45(d)(2) and 45(d)(3) provide a nonparty subpoena recipient with two separate and distinct procedural vehicles for asserting objections to a subpoena. One is not dependent upon or tied to the other. One must be filed within fourteen days of receipt; the other must merely be "timely," ordinarily meaning filed before the date set in the subpoena for compliance.⁷²

^{72.} Arthur J. Gallagher & Co. v. O'Neill, Civ. A. No. 17-2825, 2017 WL 5713361, at *1-*2, *4 (E.D. La. Nov. 27, 2017) (emphasis in original; citation omitted); accord Monitronics Int'l, Inc. v. iControl Networks, Inc., No. 3:13-mc-134-L-BN, 2013 WL 6120540, at *1 (N.D. Tex. Nov. 21, 2013) ("Rule 45 does not define a 'timely motion' but does provide that, if the subpoenaed party chooses to serve objections instead of moving to quash, '[t]he objection must be served before the earlier of the time specified for compliance or fourteen days after the subpoena is served.' Fed. R. Civ. P. 45(c)(2)(B).").

On a rule 45(d)(3)(A) motion to quash or modify a subpoena, the moving party has the burden of proof.⁷³ "Generally, modification of a subpoena is preferable to quashing it outright."⁷⁴

On a motion asserting undue burden "[t]he moving party has the burden of proof to demonstrate 'that compliance with the subpoena would be unreasonable and oppressive."⁷⁵ "The moving party opposing discovery must show how the requested discovery was overly broad, burdensome, or oppressive by submitting affidavits or offering evidence revealing the nature of the burden."⁷⁶

"Whether a burdensome subpoena is reasonable 'must be determined according to the facts of the case,' such as the party's need for the documents and the nature and importance of the litigation."⁷⁷ "To determine whether the subpoena presents an undue burden, [the Court] consider[s] the following factors: (1) relevance of the information requested; (2) the need of the party for the documents; (3) the breadth of the document request; (4) the time period covered by the request; (5) the particularity with which the party describes the requested documents; and (6) the burden imposed." *Wiwa*, 392 F.3d at 818 (footnote omitted). "Further, if the person to whom the document request is made is a nonparty, the court may also consider the expense and inconvenience to the nonparty."⁷⁸

When "a subpoena is issued as a discovery device, relevance for purposes of the undue burden test is measured according to the standard of [Federal Rule of Civil Procedure] 26(b)(1)."⁷⁹ This is because discovery from a third party as permitted through a subpoena issued under rule 45 is limited to the scope of discovery permitted under

- 76. Andra Group, LP v. JDA Software Group, Inc., 312 F.R.D. 444, 449 (N.D. Tex. 2015).
- 77. Wiwa, 392 F.3d at 818 (internal quotation marks and footnote omitted).

78. Wiwa, 392 F.3d at 818 (footnote omitted); accord Positive Black Talk Inc. v. Cash Money Records, Inc., 394 F.3d 357, 377 (5th Cir. 2004) ("Fed. R. Civ. P. 45 provides that a court shall quash (or modify) a subpoena if it 'subjects a person to undue burden.' Fed. R. Civ. P. 45(c)(3)(A)(iv). Whether a subpoena subjects a witness to undue burden generally raises a question of the subpoena's reasonableness, which 'requires a court to balance the interests served by demanding compliance with the subpoena against the interests furthered by quashing it.' 9A Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure § 2463 (2d ed. 1995). '[T]his balance of the subpoena's benefits and burdens calls upon the court to consider whether the information is necessary and unavailable from any other source.'''); abrogated by Reed Elsevier, Inc. v. Muchnick, 559 U.S. 154 (2010).

79. Williams, 178 F.R.D. at 110.

^{73.} See Wiwa v. Royal Dutch Petroleum Co., 392 F.3d 812, 818 (5th Cir. 2004); Williams v. City of Dallas, 178 F.R.D. 103, 109 (N.D. Tex. 1998).

^{74.} Wiwa, 392 F.3d at 818.

^{75.} Wiwa, 392 F.3d at 818 (quoting Williams, 178 F.R.D. at 109 (internal quotation marks omitted)).

Discovery of ESI from Nonparties

Rule 26(b)(1) in the underlying action, and "[d]iscovery outside of this scope is not permitted."⁸⁰ The provisions and structure of rules 26 and 45 indicate that the scope of permissible discovery from a third party is not broader than the scope permissible from an actual party to the suit.⁸¹

Because "[t]he scope of discovery is the same under both Federal Rules of Civil Procedure 45 and 26,"⁸² courts apply the rule 26(b)(1) proportionality factors in the context of a rule 45(d)(3)(A) motion to quash or a rule 45(d)(2)(B)(i) motion to compel or, for that matter, in the context of rule 45(d)(1)'s duty to avoid imposing undue burden or expense on a person subject to the subpoena.⁸³ And, as one judge in the Fifth Circuit has noted, where "nonparties have greater protections from discovery ... burdens on nonparties will impact the proportionality analysis."⁸⁴

The Court also "may find that a subpoena presents an undue burden when the subpoena is facially overbroad."⁸⁵ "Courts have found that a subpoena for documents from a nonparty is facially overbroad where the subpoena's document requests seek

81. See Waters v. Lincoln Gen'l Ins. Co., Civ. A. No. 07-3183, 2008 WL 659471, at *2 (E.D. La. Mar. 5, 2008) ("The scope of discovery with respect to nonparties under rule 45 is no broader than that prescribed for parties under rule 26(b)(1)."); cccord Wiwa, 392 F.3d at 818 ("Further, if the person to whom the document request is made is a nonparty, the court may also consider the expense and inconvenience to the nonparty." (footnote omitted) (citing Williams, 178 F.R.D. at 109 ("The status of a witness as a nonparty entitles the witness to consideration regarding expense and inconvenience"), which cited Concord Boat Corp. v. Brunswick Corp., 169 F R.D. 44, 49 (S.D.N.Y. 1996) ("In addition, the status of a witness as a nonparty to the underlying litigation 'entitles [the witness] to consideration regarding expense and inconvenience.""), which cited Fed. R. Civ. P. 45(c)(2)(B) and Semtek Int'l, Inc. v. Merkuriy Ltd., No. 3607 DRH, 1996 WL 238538, at *2 (N.D.N.Y. May 1, 1996) ("Second, Lockheed is a nonparty. While this status does not relieve Lockheed of its obligations either to respond to proper discovery requests or to comply with the applicable rules, it does entitle Lockheed to consideration regarding expense and inconvenience."))); cf. Am. Fed'n of Musicians of the U.S., 313 F.R.D. at 45 ("The Court finds that applying the standards of rule 26(t)(1), as amended, to the Subpoena and [the plaintiff's] motion to compel is both just and practicable where [a party] is not entitled to enforce its Subpoena against a nonparty based on a greater scope of relevance than should apply to any discovery against any party going forward.").

82. Garcia, 2017 WL 187577, at *2.

83. See Am. Fed'n of Musicians of the U.S., 313 F.R.D. at 44-45.

84. Hume v. Consolidated Grain & Barge Inc., Civ. A. No. 15-935, 2016 WL 7385699, at *3 (E.D. La. Dec. 21, 2016) (quoting E. Laporte and J. Redgrave, A Practical Guide to Achieving Proportionality Under New Federal Rule of Civil Procedure 26, 9 Fed. Cts. L. Rev. 19, 57 (2015)).

85. Wiwa, 392 F.3d at 818 (footnote omitted).

^{80.} Garcia v. Professional Contract Servs., Inc., No. A-15-cv-585-LY, 2017 WL 187577, at *2 (W.D. Tex. Jan. 17, 2017); see also Arthur J. Gallagher & Co., 2017 WL 5713361, at *2 (explaining that "subpoenas duces tecum are discovery devices governed by rule 45 but also subject to the parameters established by rule 26" and that a "court retains discretion to decline to compel production of requested documents when the request exceeds the bounds of fair discovery, even if a timely objection has not been made" (internal quotation marks omitted)).

. . . .

all documents concerning the parties to [the underlying] action, regardless of whether those documents relate to that action and regardless of date; [t]he requests are not particularized; and [t]he period covered by the requests is unlimited.⁸⁶

§ 21.9:3 Production of ESI

If the subpoena requires only the production of ESI without accompanying testimony, the nonparty must produce it at a location within one hundred miles of where he resides, is employed, or regularly transacts business in person.⁸⁷ When only production without a deposition is requested, the nonparty need not personally appear at that location to produce the ESI.⁸⁸

If the subpoena requires production along with a deposition, the deposition must be within that same 100-mile radius or anywhere in the nonparty's state if the subpoena is for trial testimony and the nonparty would not incur substantial expense.⁸⁹

As explained above, the request for ESI "may" specify the form in which it is to be produced.⁹⁰ If the subpoena does not, the nonparty must produce the ESI in the form in which it is ordinarily maintained or in a reasonably usable form.⁹¹ Only one form of the ESI need be produced.⁹²

§ 21.9:4 Costs of Production

Federal rule 45(e)(1)(D) is virtually identical to federal rule 26(b)(2)(B) and governs the procedure for discovering ESI from a nonparty that is not reasonably accessible because of undue burden or cost. Both rules provide that the person responding to the request—

need not provide discovery of electronically stored information from sources that the [person/party] identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a

- 87. Fed. R. Civ. P. 45(c)(2)(A).
- 88. Fed. R. Civ. P. 45(d)(2)(A).
- 89. Fed. R. Civ. P. 45(c)(1).
- 90. Fed. R. Civ. P. 45(a)(1)(C).
- 91. Fed. R. Civ. P. 45(e)(1)(B).
- 92. Fed. R. Civ. P. 45(e)(1)(C).

^{86.} Am. Fed'n of Musicians of the U.S., 313 F.R.D. at 45 (internal quotation marks omitted).

protective order, the [person/party] from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of rule 26(b)(2)(C). The court may specify conditions for the discovery.⁹³

This rule has been described as establishing a "two-tier approach" to discovery cf ESI.⁹⁴ A cost-benefit analysis is applied in the first instance with regard to whether the ESI should be discoverable. That analysis is applied in the second instance when the court considers how the cost of retrieval of discoverable information will be apportioned among the requesting and responding parties.

Unlike the Texas rules for discovery from nonparties, the federal approach specifically provides that the cost-shifting analysis applies to requests for production from both parties (rule 26) and nonparties (rule 45). Another important difference between the Texas rule and its federal counterpart is that in Texas, the cost of producing ESI that is not reasonably accessible but still discoverable must be borne by the requesting party.

While the Texas rule does not have an explicit requirement for showing "good cause" in order to obtain production of ESI that is not reasonably accessible, the Texas Supreme Court has derived a substantively identical standard from another rule cf civil procedure.⁹⁵

§ 21.10 Rule 27—Depositions to Perpetuate Testimony

The federal analogue to Texas rule 202 governing presuit depositions is federal rule 27; on the federal level, this mechanism is referred to as a "deposition to perpetuate testimony." Again, because no suit is actually pending, any such discovery is technically from a nonparty.

^{93.} Fed. R. Civ. P. 26(b)(2)(B), 45(e)(1)(C).

^{94.} These two tiers are (1) the designation by the responding party that the ESI requested is "not reasonably accessible" and (2) the hearing and showing required to resist discovery of ESI not reasonably accessible.

^{95.} Weekley Homes, 295 S.W.3d at 317; Tex. R. Civ. P. 192.4(b).

§ 21.10

§ 21.10:1 Petition for Deposition to Perpetuate Testimony

The person wishing to take a deposition to perpetuate testimony must petition a court for permission to do so. This petition must include an explanation of the subject matter of the suit and the reason it cannot presently be brought, as well as an identification of the adverse parties and deponent, the expected substance of the testimony to be elicited, and the reasons for perpetuating that testimony.⁹⁶

The petition must be verified and should be filed in the district court for the district in which any expected adverse party resides.⁹⁷

§ 21.10:2 Notice of Hearing on Petition

Notice of the hearing on the petition for presuit discovery must be made on the deponent and adverse parties at least twenty-one days before the date of the hearing.⁹⁸ The notice must be served under rule 4, the standard rule for service applicable to most filings.⁹⁹ The court may order service by publication under appropriate circumstances, but must appoint an attorney to represent the potential party served by publication, who may cross-examine the deponent.¹⁰⁰

§ 21.10:3 Applicability of Rules for Nonparty Discovery

Though not as specifically prescribed as its Texas equivalent, the conduct of a deposition to perpetuate testimony is governed by rule 34, which in turn invoked rule 45 for nonparties.¹⁰¹ Thus, the form of the presuit deposition notice, its contents, and the timing of its service all follow the rules discussed above.

§ 21.11 Rule 45—Entry on Property for Inspection

The court's order must state the manner, conditions, and scope of the inspection and must specifically describe any desired means, manner, and procedure for testing or

- 98. Fed. R. Civ. P. 27(a)(2).
- 99. Fed. R. Civ. P. 27(a)(2), (a)(4).
- 100. Fed. R. Civ. P. 27(a)(2), (a)(4).
- 101. Cf. Fed. R. Civ. P. 27(a)(3), Tex. R. Civ. P. 202.5.

^{96.} Fed. R. Civ. P. 27(a)(1).

^{97.} Fed. R. Civ. P. 27(a)(1).

Discovery of ESI from Nonparties

sampling.¹⁰² Therefore, the party requesting this discovery mechanism should ensure that provisions for the production of any ESI that is created be included in that order.

§ 21.12 Rule 35—Physical and Mental Examinations

Discovery requests for physical and mental examinations are governed by rule 35. Unlike in the Texas rules, there is no specific provision in either rule 35 or rule 45 permitting the court to order a nonparty to submit to such an examination.

§ 21.13 Conclusion

Under both Texas and federal procedural rules, there are three primary means of acquiring ESI from nonparties: subpoenas, depositions taken before suit is filed, and tests conducted while present on real property. Texas recognizes a fourth category of nonparty discovery, with ESI produced during a physical or mental examination.

The rules for employing each of these procedures are nuanced and differ in the state and federal schema, sometimes markedly. Both the federal and state rules, however, emphasize the need to prevent undue burden upon a nonparty. Furthermore, the applicability of other standards developed with respect to the discovery of ESI from the parties themselves—such as cost-shifting—must also be considered when seeking nonparty discovery.

102. Tex. R. Civ. P. 196.7(b).



Chapter 22

Introduction to Computer Forensics

Craig Ball

§ 22.1 What Is Computer Forensics?

A computer's operating system or OS (e.g., Windows, Mac, or Linux) and its installed software or applications generate and store much more information than users realize. Some of this unseen information is active data readily accessible to users, but sometimes it requires skilled interpretation to be of value in illuminating human behavior. Examples include the data about data, or metadata, tracked by the operating system and applications. For example, Windows Explorer supports the display of geolocation data embedded within cell phone photos, but few users customize their folder view to reveal such information.

Other active data resides in obscure locations or in encoded formats not readily accessible or comprehensible to users, but enlightening when interpreted and correlated by forensic examiners or others with proper software and training. Log files, hidden system files, and information recorded in nontext formats are examples of encoded data that may reveal information about user behavior. To illustrate, in a data theft investigation, crucial evidence may reside within the system registry as time-stamped entries logging when USB storage devices were first and most recently attached to an employee's laptop.

Finally, there are vast regions of hard drives and other data storage devices that hold forensic artifacts in areas and forms that even the operating system can't access. These digital boneyards, called "unallocated clusters" and "slack space," contain much of what a user, application, or OS discards over the life of a machine. Accessing and making sense of these vast, unstructured troves demands the specialized tools, techniques, and skill of a computer forensics examiner and may produce the most compelling evidence in a case, particularly in cases of suspected spoliation.

Computer forensics is the expert acquisition, interpretation, and presentation of the data within the three categories (active, encoded, and forensic data), along with its juxtaposition against other available information (e.g., credit card transactions, key-

card access data, phone records, social networking, voice mail, e-mail, documents, and text messaging).

In litigation, computer forensics isn't limited to personal computers and servers but may extend to all manner of devices harboring electronically stored information ("ESI"). Certainly, external hard drives, thumb drives, and memory cards are routinely examined, and, increasingly, relevant information resides on phones, tablets, cameras, IoT devices, and even automobile navigation systems and air bag deployment modules. The scope of computer forensics—like the scope of a crime scene investigation—expands to mirror the available evidence and issues before the court.

§ 22.2 How Does Computer Forensics Differ from Electronic Discovery?

Computer forensics is a nonroutine subcategory of e-discovery. In simplest terms, electronic discovery addresses the ESI accessible to litigants; computer forensics addresses the ESI accessible to forensic experts. However, the lines blur because e-discovery often requires litigants to grapple with forms of ESI deemed not reasonably accessible due to burden or cost, and computer forensic analysis often turns on information readily accessible to litigants, such as file modification dates.

The principal differentiators are (1) expertise (computer forensics requires a unique skill set), (2) issues (most cases can be resolved without resorting to computer forensics, though some will hinge on matters that can only be resolved by forensic analysis), and (3) proportionality (computer forensics injects issues of expense, delay, and intrusion). Additionally, electronic discovery tends to address evidence as discrete information items (documents, messages, databases), while computer forensics takes a more systemic or holistic view of ESI, studying information items as they relate to one another and in terms of what they reveal about what a user did or tried to do. And last but not least, electronic discovery deals almost exclusively with existing ESI; computer forensics frequently focuses on what's gone, how and why it's gone, and how it might be restored.

§ 22.3 When to Turn to Computer Forensics

Most cases require no forensic-level computer examination, so parties and courts should closely probe whether a request for access to an opponent's machines is grounded on a genuine need or is simply a fishing expedition. When the question is close, courts can balance need and burden by using a neutral examiner and a protective protocol, as well as by assessing the cost of the examination against the party seeking same until the evidence supports reallocation of that cost.

Certain disputes demand forensic analysis of relevant systems and media, and, in these cases, the parties and/or the court should act swiftly to support appropriate efforts to preserve relevant evidence. For example, claims of data theft may emerge when a key employee leaves to join or become a competitor, prompting a need to forensically examine the departing employee's current and former business machines, portable storage devices and home machines. Such examinations inquire into the fact and method of data theft and the extent to which the stolen data has been used, shared, or disseminated.

Cases involving credible allegations of destruction, alteration, or forgery of ESI also justify forensic analysis, as do matters alleging system intrusion or misuse, such as instances of employment discrimination or sexual harassment involving the use of electronic communications. Of course, electronic devices now figure prominently in the majority of crimes and domestic relations matters, too. It's the rare fraud or dalliance that doesn't leave behind a trail of electronic breadcrumbs in e-mail, messaging, online financial histories, and mobile devices.

§ 22.4 What Can Computer Forensics Do?

Though the extent and reliability of information gleaned from a forensic examination varies, here are some examples of the information an analysis may uncover:

- Manner and extent of a user's theft of proprietary data
- Timing and extent of file deletion or antiforensic (e.g., data wiping) activity
- Whether and when a thumb drive or external hard drive was connected to a machine
- Forgery or alteration of documents
- Recovery of deleted ESI, file structures, and associated metadata
- Internet usage, online activity, cloud storage access, and e-commerce transactions
- Intrusion and unauthorized access to servers and networks
- Social networking

- Clock and calendar tampering
- Photo manipulation
- Minute-by-minute system usage

§ 22.5 What Can't Computer Forensics Do?

Notwithstanding urban legend and dramatic license, there are limits on what a computer forensic examination can accomplish. To illustrate, an examiner generally cannot—

- 1. recover any information that has been completely overwritten—even just once—by new data;
- 2. conclusively identify the hands on the keyboard if one person logs in as another;
- 3. conduct a thorough forensic examination without access to the evidence media or a forensically sound image of same;
- recover data from a drive that has suffered severe physical damage and cannot spin;
- 5. guarantee that a drive won't fail during the acquisition process; or
- 6. rely upon any software tool to autonomously complete the tasks attendant to a competent examination; that is, "pushbutton forensics" doesn't exist.

§ 22.6 Balancing Need, Privilege, and Privacy

A computer forensic examiner sees it all. The Internet has so broken down barriers between business and personal communications that workplace computers are routinely peppered with personal, privileged, and confidential communications, even intimate and sexual content, and personal devices routinely hold business data. Further, a hard drive is more like one's office than a file drawer. It may hold data about the full range of a user's daily activity, including private or confidential information, and teem with trade secrets, customer data, e-mail flirtations, salary schedules, Internet searches for pornography and escort services, bank account numbers, online shopping, medical records, and passwords.

So how does the justice system afford access to discoverable information without inviting abuse or exploitation of the rest? With so much at stake, parties and the courts

must approach forensic examination cautiously. Access should hinge on demonstrated need and a showing of relevance, balanced against burden, cost, or harm. Direct access to storage media should be afforded an opponent only when, for example, it's been demonstrated that an opponent is untrustworthy, incapable of preserving and producing responsive information or that the party seeking access has some proprietary right with respect to the drive or its contents. Showing that a party lost or destroyed ESI is a common basis for access, as are situations like sexual harassment or data theft where the computer was instrumental to the alleged misconduct.

In Texas, the process attendant to seeking forensic examination is described by the Texas Supreme Court in *In re Weekley Homes, L.P.,* 295 S.W.3d 309 (Tex. 2009), a dispute concerning a litigant's right to directly access an opponent's storage media. The plaintiff wanted to run twenty-one search terms against the hard drives of four of defendant's employees in an effort to find deleted e-mails. The standards that emerged from the court's remand serve as a sensible guide to those seeking to compel an opponent to recover and produce deleted e-mail, to wit:

- 1. Parties seeking production of deleted e-mails should specifically request them and specify a form of production.
- 2. Responding parties must produce reasonably available information in the format sought. They must object if the information is not reasonably available or if they oppose the requested format.
- 3. Parties should try to resolve disputes without court intervention; but if they can't work it out, either side may seek a hearing at which the responding party bears the burden to prove that the information sought is not reasonably available because of undue burden or cost.
- 4. If the trial court determines the requested information is not reasonably available, the court may still order production if the requesting party demonstrates that it's feasible to recover deleted, relevant materials and the benefits of production outweigh the burden, for example, the responding party's production is inadequate absent recovery.
- 5. Direct access to another party's storage devices is discouraged; but, if ordered, only a qualified expert should be afforded such access, subject to a reasonable search and production protocol protecting sensitive information and minimizing undue intrusion.
- 6. The requesting party pays the reasonable expenses of any extraordinary steps required to retrieve and produce the information

In Weekley Homes, the Supreme Court further articulated a new duty:

Early in the litigation, parties must share relevant information concerning electronic systems and storage methodologies to foster agreements regarding protocols and equip courts with the information needed to craft suitable discovery orders.

In re Weekley Homes, 295 S.W.3d at 321. That's a familiar—though poorly realized—obligation in federal practice, but one largely absent from state court practice nationwide.

Weekley Homes brings much-needed discipline to the process of getting to the other side's drives, but scant guidance about what's required to demonstrate feasible recovery of deleted e-mail or what constitutes a proper protocol to protect privilege and privacy. Something that seems simple to counsel can enormously complicate forensic examination and recovery, at great cost. A sensible protocol balances what lawyers want against what forensic experts can deliver.

The parties may agree that one side's computer forensics expert will operate under an agreed protocol to protect unwarranted disclosure of privileged and confidential information. Increasingly, federal courts appoint neutral forensic examiners to serve as rule 53 special masters for the purpose of performing the forensic examination *in camera*. To address privilege concerns, the information developed by the neutral may first be tendered to counsel for the party proffering the devices, who then generates a privilege log and produces nonprivileged, responsive data.

Whether an expert or court-appointed neutral conducts the examination, the order granting forensic examination of ESI should provide for handling of confidential and privileged data and narrow the scope of examination by targeting specific objectives. The examiner needs clear direction in terms of relevant keywords and documents, as well as pertinent events, topics, persons, and time intervals. A common mistake is for parties to agree upon a search protocol or secure an agreed order without consulting an expert to determine feasibility, complexity or cost. Generally, use of a qualified neutral examiner is more cost-effective and ensures that the court-ordered search protocol is respected.

§ 22.7 Who Performs Computer Forensics?

Though the ranks of those offering computer forensics services are growing, there is spotty assessment or regulation of the profession. Only a handful of respected certifi-

Introduction to Computer Forensics

cations exist to test the training, experience, and integrity of forensic examiners. These include the certified computer examiner (CCE), certified forensic computer examiner (CFCE), and encase certified examiner (EnCE). Some states require computer forensic examiners to obtain private investigator licenses, but don't demand that applicants possess or demonstrate expertise in computer forensics.

Computer experts without formal forensic training or experience may also offer their services as experts; but just as few doctors are qualified as coroners, few computer experts are qualified to undertake a competent digital forensics analysis. Programming skill has little practical correlation to skill in computer forensics.

§ 22.8 Drafting Digital Examination Protocols

A computer or smart phone under forensic examination is like a vast metropolis of neighborhoods, streets, buildings, furnishings, and loads of stuff. It's customary for a single machine to yield over a million discrete information items, some items holding thousands of data points. Searching so vast a virtual metropolis requires a clear description of what's sought and a sound plan to find it.

In the context of electronic discovery and digital forensics, an examination protocol is an order of a court or an agreement between parties that governs the scope and procedures attendant to testing and inspection of a source of electronic evidence. Parties and courts use examination protocols to guard against compromise of sensitive or privileged data and insure that specified procedures are employed in the acquisition, analysis, and reporting of electronically stored information.

A well-conceived examination protocol serves to protect the legitimate interests of all parties, curtails needless delay and expense, and forestalls fishing expeditions. Protocols may afford a forensic examiner broad leeway to adapt procedures and follow the evidence, or a protocol may tightly constrain an examiner's discretion to defend against waiver of privilege or disclosure of irrelevant, prejudicial material. A good protocol helps an examiner know where to start his or her analysis, how to proceed, and, crucially, when the job is done.

As a litigator for over thirty-five years and a computer forensic examiner for more than twenty-five years, I've examined countless devices and sources for courts and litigants. In that time, I've never encountered a forensic examination protocol of universal application. "Standard" procedures change over time, adapted to new forms of digital evidence and new hurdles, like full-disk encryption, solid-state storage, and explosive growth in storage capacities and data richness. Without a protocol, a forensics examiner could spend months seeking to meet an equivocal examination mandate. The flip side is that poor protocols damn examiners to undertake pointless tasks and overlook key evidence.

Drafting a sensible forensic examination protocol demands a working knowledge of the tools and techniques of forensic analysis so counsel doesn't try to misapply e-discovery methodologies to forensic tasks. Forensic examiners deal in artifacts, patterns, and configurations. The data we see is structured and encoded much differently than what a computer user sees. The significance and reliability of an artifact depends on its context. Dates and times must be validated against machine settings, operating system functions, time zones, and corroborating events.

Much in digital forensics entails more than meets the eye; consequently, simply running searches for words and phrases "e-discovery-style" is far less availing than it might be in a collection of documents.

If you can conceive of taking the deposition of a computer or smart phone, crafting a forensic examination protocol is like writing out the questions in advance. Like a deposition, there are basic inquiries that can be scripted, but no definitive template for follow-up questions. A good examiner—of people or computers—follows the evidence, yet hews to relevant lines of inquiry and respects boundaries. A key difference is that good advocates fit the evidence to their clients' narrative, whereas good forensic examiners let the evidence tell its own story.

If you've come here for a form examination protocol, you'll find it; but the "price" is learning a little about why forensic examination protocols require certain language, and above all, why you must carefully adapt any protocol to the needs of your case.

§ 22.8:1 Common Elements

Though each is unique, examination protocols share common elements. They should, inter alia—

- identify the examiner (or the selection process) and the devices and media under scrutiny;
- set the scope of the exam, temporally and topically;
- ensure integrity of the evidence;
- detail the procedures and analyses to be completed;

- set deadlines and reporting responsibilities;
- require cooperation; and
- assign payment duties.

Protocols typically set out the goals of the exam and articulate the rights sought to be protected. As needed, a protocol should address the who, what, when, and where of access to devices or media and the conditions under which acquisition and examination will occur. A proper chain of custody is mandated, as well as who may be present when data is acquired or processed.

§ 22.8:2 Identify Examiner

If a neutral will perform the exam, ideally the parties will agree on a qualified person. When they cannot, the court may seek recommendations from other judges before whom well-qualified examiners have appeared, or the protocol can require each side to submit proposed candidates, including their curriculum vitae and a list of other matters in which the examiner candidates have served as court-appointed neutrals. The court then reviews the CVs for evidence of training, experience, credible professional certification, and other customary indicia of expertise in selecting its appointee. The protocol should make clear whether the examiner is working for a party or serving as a neutral.

Exemplar language: The parties have until [Date] to agree upon a computer forensic examiner ("Examiner") who will inspect and analyze the electronic devices and media pursuant to this Protocol. If the parties fail to agree on an Examiner, they shall submit two names each to the Court with a summary of the proposed Examiners' qualifications and experience, not to exceed one page each, and each Examiner's fee structure. The Court will select an Examiner from among the candidates submitted. The Examiner will serve as an officer of the court, agree to submit to the jurisdiction of this Court and be bound by the terms of this Protocol.

§ 22.8:3 Identify Devices and Media

A forensic examination protocol should clearly define what devices and media must be tendered for acquisition and analysis. Designations may be as specific as "Dell Inspiron laptop computer Service Tag XYZ123" or as broad as "all computers, cell phones, and electronic data storage devices (thumb drives, external hard drives, and the like) in the care custody or control of John Doe." Forensic examinations routinely turn up evidence pointing to the existence of other potentially relevant devices and storage media. This triggers mistrust and charges of concealment or spoliation. Accordingly, the parties should discuss the potential for other devices to turn up and draft the examination protocol to address whether such items fall within the scope of the examination.

§ 22.8:4 Set Scope of Examination

As noted, there is no more a standard protocol applicable to every forensic examination than there is a standard set of deposition questions applicable to every matter or witness. In either circumstance, a skilled examiner tailors the inquiry to the case, follows the evidence as it develops and remains flexible enough to adapt to unanticipated discoveries. Consequently, it is desirable for a court-ordered protocol to afford the examiner some discretion to adapt to the evidence and apply their expertise.

In framing a forensic examination order, it's helpful to set out the goals to be achieved and the risks to be averted. By using an aspirational statement to guide the overall effort instead of directing the details of the expert's forensic activities, the parties and the court reduce the risk of a costly, wasteful exercise. To illustrate, a protocol might state: "The computer forensic examiner should, as feasible, recover and produce from Smith's computer, phone, and storage media tendered for examination all e-mail communications between John Smith and Jane Doe, but without revealing Smith's personal confidential information or the contents of privileged attorney-client communications to any person other than Smith's counsel."

The court issued a clear, succinct order in *Bro-Tech Corp. v. Thermax, Inc.*, No. 05-CV-2330, 2008 WL 724627, at *5 (E.D. Pa. Mar. 17, 2008). Though it assumed some existing familiarity with the evidence (e.g., referencing certain "Purolite documents"), an examiner should have no trouble understanding what was expected:

- (1) Within three (3) days of the date of this Order, Defendants' counsel shall produce to Plaintiffs' computer forensic expert forensically sound copies of the images of all electronic data storage devices in Michigan and India of which Huron Consulting Group ("Huron") made copies in May and June 2007. These forensically sound copies are to be marked "CONFIDENTIAL—DESIGNATED COUNSEL ONLY";
- (2) Review of these forensically sound copies shall be limited to:

(a)

§ 22.8

- such in this litigation;
- (b) file name searches for the Purolite documents; and
- (c) searches for documents containing any term identified by Stephen C. Wolfe in his November 28, 2007 expert report;
- (3) All documents identified in these searches by Plaintiffs' computer forensic expert will be provided to Defendants' counsel in electronic format, who will review these documents for privilege;
- (4) Within seven (7) days of receiving these documents from Plaintiffs' computer forensic expert, Defendants' counsel will provide all such documents which are not privileged, and a privilege log for any withheld or redacted documents, to Plaintiffs' counsel. Plaintiffs' counsel shall not have access to any other documents on these images;
- (5) Each party shall bear its own costs.

Of course, this order keeps a tight rein on the scope of examination by restricting the effort to hash value, filename, and keyword searches. Such limitations are appropriate where the parties are seeking a small population of well-known documents but would severely hamper a less-targeted effort. It bears mention that the *Bro-Tech* protocol was barely a forensic examination as it focused exclusively on active data, not forensic artifacts. As such, it's a poor template for a deeper inquiry.

§ 22.8:5 Set Temporal Scope

Parties routinely seek to impose time constraints on a forensic examination in terms of what data the examiner should search. While limiting an examiner to review of information in a relevant interval may seem wise, it's often infeasible and serves to frustrate the ends of the exam. No forensics tool can limit a search of unallocated clusters and forensic artifacts to a date range. There are few temporal guideposts for forensic artifacts because date information is usually absent or may be unreliable. Even for active data, there won't always be metadata in the master file table to support a reliable time limitation.

For example, log files contain information pertaining to dates other than the dates cf the log files themselves. Excluding log files based on their file dates serves to prevent scrutiny of temporally relevant log entries. Moreover, file metadata misleads those who don't fully understand its significance. A file's creation date often bears no relation to the date the file's contents were authored. A file's last modified date may relate

to events outside a relevant interval although the contents of the file are precisely what the parties seek. An examiner can limit the date range only for items that have

So, be wary of language like, "All searches are restricted to the time period from November 1, 2018, through May 23, 2019." Interval limitations on search don't fly, and you won't know what you're missing.

A preferable approach in a protocol might be to specify that the examiner should not produce information to counsel if the examiner determines that the information falls outside of the relevant interval specified in the protocol. The distinction is that, while an examiner may not be able to limit a search to an interval, an examiner can often glean enough information about items found to make a reasonable assessment of their temporal relevance.

Exemplar Language: The parties intend that the scope of the examination be, as feasible, limited to the Relevant Interval: [Date 1] through [Date 2]. Except as otherwise specified herein, Examiner should make reasonable efforts to exclude from production the information that the Examiner determines falls outside of the Relevant Interval.

§ 22.8:6 Assess Evidence Integrity

reliable temporal metadata, but not otherwise.

If you're seeking a forensic exam, there's a good chance you suspect fraud or spoliation. It should come as no surprise to learn that evidence tendered for forensic examination is often swapped, fabricated, sterilized, reformatted, reimaged, or otherwise corrupted. Why then do so many lawyers framing examination protocols fail to explicitly require that the integrity of the evidence be assessed?

A threshold step in any forensic examination should include consideration of whether the evidence supplied is what it purports to be and if its contents have been wiped or manipulated to subvert the exam.

Exemplar Language: The Examiner shall assess the integrity of the evidence by, e.g., checking Registry keys to investigate the possibility of drive swapping or fraudulent reimaging and looking at logs to evaluate BIOS clock manipulation. The Examiner may take other reasonable steps to determine if the data supplied is consistent with its stated origins, including but not limited to:

- 1. looking at the dates of key system folders to assess temporal consistency with the device, operating system, and events;
- 2. looking for instances of applications employed to alter file metadata or erase/alter system cache and history data; and
- 3. noting the presence and nature of any recently installed applications and/or antiforensic "privacy" tools.

The Examiner shall promptly report any irregularities concerning the integrity of the evidence to counsel for the parties.

§ 22.8:7 Provide for Cooperation

Hardened device security has made it difficult for computer forensic examiners to forgo passwords and bypass encryption. Today it's common that users must supply their access credentials to facilitate examination. A good examination protocol obliges parties to promptly supply same on request.

Exemplar Language: The Parties shall cooperate with the Examiner insofar as promptly supplying nonprivileged information and passwords and credentials required to access and decrypt data on the Image and accurately interpret same. No passwords or credentials obtained from the image or furnished by the parties will be used by the Examiner to access data other than found on the Image.

§ 22.8:8 Plot the Process

The most daunting feature of a forensic examination protocol is detailing the procedures and analyses to be completed. It's important to lay out these steps because forensic examiners use different tools, call things by different names, and don't all possess the same grasp of forensic artifacts and their significance. The best way to ensure that the work gets done is to describe what's required in language the examiner will clearly understand and steps the examiner has the tools and expertise to complete.

You can't do that by blindly borrowing language from a protocol from a different case. Instead, read up on common forensic artifacts or, better yet, consult a forensic examiner to lay out what needs to be done, describing the steps in enough detail that any examiner using one of the leading forensic tools will know what to do and where to look.

The single biggest mistake lawyers make in drafting forensic examination protocols is requiring examiners to do things they can't do. Forensic examiners can't always tell what files a user copied or what files were deleted. We can't always tell who logged in using another's password. Despite what you see on television, computers don't track everything, and they don't simply log all events, even in the event logs.

Forensics is a powerful tool, but it's not magic. Most forensic artifacts on which examiners rely exist only by way of happy accidents.

§ 22.9 How Windows Deletes a File

Windows can be downright obstinate in its retention of data that you don't want to hang around. Neither emptying the Recycle Bin nor performing a quick format of a disk will obliterate all its secrets. How is that deleting a file doesn't, well, *delete* it? The answer lies in how Windows stores and catalogs files. Remember that the Windows files system deposits files at various locations on your disc drive and then keeps track of where it has tucked those files away in its master file table (MFT)—the table of contents for the massive tome of data on your drive.

The MFT keeps tabs on what parts of the hard drive contain files and what parts are available for storing new data. When you delete a file, Windows doesn't scurry around the hard drive vacuuming up 1s and 0s. Instead, all it does is add an entry to the master file table that tells the system "this file has been deleted" and, by so doing, makes the disk space containing the deleted data (called "unallocated space") available for storage of new data. But deciding that a file drawer can be used for new stuff and clearing out the old stuff are two very different things. The old stuff—the deleted data—stays on an electromagnetic hard drive until new data overwrites it.

If we return to our library card catalog analogy, pulling a card from the card catalog doesn't remove the book from the shelf, though consulting the card catalog you wouldn't know it's there. Deleting a computer file only removes its "card" (the file table record). The "book" (the file's content) hangs around until the librarian needs the shelf space for new titles.

Let's assume there is a text file called "accounts.txt" on your computer and it contains the account numbers and passwords for your offshore numbered accounts. Let's assume that the bloom has gone off the rose that was your marriage and you decide that maybe it would be best to get this file out of the house. So you copy it to a thumb drive and then delete the original. Now, you're probably aware that though the file no longer appears in its folder, it's still accessible in the Recycle Bin. Consequently, you open the Recycle Bin and execute the "Empty Recycle Bin" command, thinking you can now rest easy. In fact, the file is not gone. All that has occurred is that Windows has flipped a bit in the MFT to signal that the space once occupied by the file is now available for reuse. The file and all of the passwords and account numbers it holds is still on the drive, and until the physical space the data occupies is overwritten by new data, it's not that hard to read the contents of the old file or undelete it. Even if the file is overwritten, there's a chance that part of its contents can be read if the new file is smaller in size than the file it replaces. This is true for your text files, financial files, images, Internet pages you've visited, and your e-mail.

§ 22.10 Happy Accidents: Files that Still Contain Data

You can roughly divide the evidence in a computer forensic examination between evidence generated or collected by a user (e.g., an Excel spreadsheet or downloaded photo) and evidence created by the system that serves to supply the context required to authenticate and weigh user-generated evidence. User-generated or -collected evidence tends to speak for itself without the need of expert interpretation. In contrast, artifacts created by the system require expert interpretation, in part because such artifacts exist to serve purposes having nothing to do with logging a user's behavior fcr use as evidence in court. Most forensic artifacts arise because of a software developer's effort to supply a better user experience and improve system performance. Their probative value in court is a happy accident.

§ 22.10:1 LNK Files, Prefetch, Windows Registry, and Other Revealing Artifacts

For example, on Microsoft Windows systems, a forensic examiner may look to machine-generated artifacts called LNK files, prefetch records and Registry keys to determine what files and applications a user accessed and what storage devices a user attached to the system. LNK files (pronounced "link" and named for their file extension) serve as pointers or "shortcuts" to other files. They are like shortcuts users create to conveniently launch files and applications, but these LNK files aren't user-created. Instead, the computer's file system routinely creates them to facilitate access to recently used files and stores them in the user's Recent folder. Each LNK file contains information about its target file that endures even when the target file is deleted, including times, size, location, and an identifier for the target file's storage medium. Microsoft didn't intend that Windows retain information about deleted files in orphaned shortcuts, but there's the happy accident—or maybe not so happy for the person caught in a lie because his computer was trying to better serve him.

Similarly, Windows seeks to improve system performance by tracking the recency and frequency with which applications are run. If the system knows what applications are most likely to be run, it can "fetch" the programming code those applications need in advance and preload them into memory, speeding the execution of the program. Thus, records of the last 128 programs run are stored in series of so-called "prefetch" files. Because the metadata values for these prefetch files coincide with use of the associated program, by another happy accident, forensic examiners may attest to, for example, the time and date a file wiping application was used to destroy evidence of data theft.

Two more examples of how much forensically significant evidence derives from happy accidents are the USBSTOR and DeviceClasses records found in the Windows System Registry hive. The Windows Registry is the central database that stores configuration information for the system and installed applications—it's essentially everything the operating system needs to "remember" to set itself up and manage hardware and software. The Windows Registry is huge and complex. Each time a user boots a Windows machine, the registry is assembled from a group of files called "hives." Most hives are stored on the boot drive as discrete files and one—the hardware hive—is created anew each time the machine inventories the hardware it sees on boot.

The registry can provide information of forensic value, including the identity of the computer's registered user, usage history data, program installation information, hard-ware information, file associations, serial numbers, and some password data. The registry is also one area where you can access a list of recent websites visited and documents created, often even if the user has taken steps to delete those footprints. A key benefit of the registry in forensics is that it tracks the attachment of USB storage media like thumb drives and external hard drives, making it easier to track and prove data theft.

When a user connects an external mass storage device like a portable hard drive or flash drive to a USB port, the system must load the proper device drivers to enable the system and device to communicate. To eliminate the need to manually configure drivers, devices have evolved to support so-called "plug and play" capabilities. Thus, when a user connects a USB storage device to a Windows system, Windows interrogates the device, determines what driver to use and—importantly—records information about the device and driver pairing within a series of keys stored in the ENUM/ USBSTOR and the DeviceClasses keys of the System Registry hive. In this process, Windows tends to store the date and time of both the earliest and latest attachments of the USB storage device.

Windows is not recording the attachment of flash drives and external hard drives to enable forensic examiners to determine when employees attached storage devices to steal data. The device programmer's goal was to speed selection of the right drivers the next time the USB devices were attached; but the happy accident is that the data retained for a non-forensic purpose carries enormous probative value when properly interpreted and validated by a qualified examiner.

§ 22.10:2 Shellbags

If you've ever wondered why after changing the size and shape of a Windows Explorer folder your preferences are retained the next time you use that folder, the answer lies in Windows retention of folder configuration data in keys (entries) within the system registry called "shellbags."

So when a forensic examiner locates a shellbag key for a folder, the examiner can reasonably conclude that the folder has been opened. This is a significant observation if the folder contains, say, child pornography or other data the user was not permitted to access.

Shellbags are also a trove of other data respecting the folder, relevant dates, and even files that formerly resided within the folder but have been moved or deleted.

§ 22.10:3 Swap and Hibernation Files

Just like you and me, Windows needs to write things down as it works to keep from exceeding its memory capacity. Wincows extends its memory capacity (RAM) by swapping data to and from a file called a "swap file." When a multitasking system such as Windows has too much information to hold in memory at once, some of it is stored in the swap file until needed. If you've ever wondered why Windows seems to always be accessing the hard drive, sometimes thrashing away for an extended period, chances are it's reading or writing information to its swap file. Windows uses the term "page file" (because the blocks of memory swapped around are called "pages"), but it's essentially the same thing: a giant digital scratch pad.

The swap file contains data from the system memory; consequently, it can contain information that the typical user never anticipates would reside on the hard drive. Moreover, we are talking about a considerable volume of information; how much varies from system to system, but it runs to billions of bytes. For example, the page file on the windows machine used to write this chapter is currently nine gigabytes in size. As to the contents of a swap file, it's pretty much a sizable (twenty-four gigabytes on my machine) swath of whatever kind of information exists (or used to exist) on a computer, running the gamut from word processing files, e-mail, Internet web pages, database entries, QuickBooks files, you name it. It also includes passwords and decryption keys. If the user used it, parts of it are floating around the swap file.

Because the memory swapping is by default managed dynamically in Windows, the swap file tends to disappear each time the system is rebooted and its contents relegated to unallocated space and recoverable in the same manner as other deleted files.

Another system file of a similar nature is the Windows hibernation file (hiberfil.sys). It records the system state when the computer hibernates to promote faster waking from sleep mode. Accordingly, it stores to disk all data from running applications at the time the machine went into hibernation mode.

Windows swap and hibernation files are forensic treasure troves, but they are no picnic to examine. Although filtering software exists to help in locating so-called "named entities," for example, passwords, phone numbers, credit card numbers, and fragments of English language text, it's still very much a labor-intensive effort (like so much of computer forensics in this day of vast hard drives).

§ 22.10:4 Windows NTFS Log File

The NTFS file system increases system reliability by maintaining a log of system activity. The log is designed to allow the system to undo prior actions if they have caused the system to become unstable. The log file is a means to reconstruct aspects of computer usage. The log file is customarily named "\$LogFile," but it is not viewable in Windows Explorer, so don't become frustrated looking for it.

§ 22.10:5 TMP Files

Every time you run Microsoft Word, Excel, PowerPoint, and other programs, these programs create temporary files. The goal of temp files is often to save your work in the event of a system failure and then disappear when they are no longer needed. Temp files do a respectable job saving your work, but, much to the good fortune of the forensic investigator, they do a lousy job of disappearing. Computers orphan temp files when a program locks up, when power fails, or due to other atypical shutdowns. When the application restarts it creates a new temp file, but rarely does away with its
orphaned predecessor. It just hangs around. Even when the application deletes the temp file the contents of the file tend to remain in unallocated space until overwritten.

As an experiment, search your hard drive for all files with the .TMP extension. You can usually do this with the search query "*.TMP." You may have to adjust your system settings to allow viewing of system and hidden files. When you get the list, forget any files with a current date and look for .TMP files from prior days.¹ Open those in Notepad or WordPad and you may be shocked to see how much of your work hangs around without your knowledge. Word processing applications are by no means the only types which keep (and orphan) temp files.

Files with the .BAK, .WBK, or .ASD extensions usually represent timed backups of works in progress maintained to protect a user in the event of a system crash or program lock up. Applications like word processing software create BAK and ASD files at periodic intervals. While these files are supposed to be deleted by the system, they often linger on.

§ 22.10:6 Volume Shadow Copies

Microsoft has been gradually integrating a feature called "Volume Snapshot Service" (a.k.a. Volume Shadow Copy Service (VSS)) into Windows since version XP, but until Windows 7 you couldn't truly say the implementation was so refined and entrenched as to permit the recovery of almost anything from a remarkable cache of data called "volume shadow copies."

Volume shadow copies are largely unknown to the e-discovery community. Though a boon to forensics, volume shadow copies may prove a headache in e-discovery because their contents represent reasonably accessible ESI from the user's standpoint.

Much of what e-discovery professionals believe about file deletion, wiping, and even encryption goes out the window when a system runs any version of Windows with Volume Snapshot Service enabled (and it's enabled by default). Volume shadow copies keep virtually everything, and Windows keeps up to sixty-four-volume shadow copies, made at daily or weekly intervals. These aren't just system restore points; volume shadow copies hold user work product, too. The frequency of shadow-copy creation varies based on multiple factors, including whether the machine is running on AC power, CPU demand, user activity, volume of data needing to be replicated, and

^{1.} I found more than 2,600 old .TMP files on my machine on May 1, 2019.

changes to system files. So sixty-four "weekly" shadow volumes could represent anywhere from two weeks to two years of indelible data, or far less.

How indelible? Consider this: most applications that seek to permanently delete data at the file level do it by deleting the file then overwriting its storage clusters. As you've learned, these are called "unallocated clusters" because they are no longer allocated to storage of a file within the Windows file system and are available for reuse. But the VSS monitors both the contents of unallocated clusters and any subsequent efforts to overwrite them. Before unallocated clusters are overwritten, VSS swoops in and rescues the contents of those clusters like Spider-Man saving Mary Jane.

These rescued clusters (a.k.a. blocks) are stored in the next created volume shadow copy on a space-available basis. Thus, each volume shadow copy holds only the changes made between shadow volume creation; that is, it records only *differences* in the volumes on a block basis in much the same way that incremental backup tapes record only changes between backups, not entire volumes. When a user accesses a previous version of a deleted or altered file, the operating systems instantly assembles all the differential blocks needed to turn back the clock. It's all just three clicks away:

- 1. Right click on file or folder for context menu
- 2. Left click to choose "Restore Previous Versions"
- 3. Left click to choose the date of the volume²

It's an amazing performance, but a daunting one for those seeking to make data disappear. From the standpoint of e-discovery, responsive data that's just three mouse clicks away is likely to be deemed fair game for identification, preservation, and production. Previous versions of files in shadow volumes are as easy to access as any other file. There's no substantial burden or collection cost for the user to access such data, item by item. But as easy as it is, few of the standard e-discovery tools and protocols have been configured to identify and search the previous versions in volume shadow copies. It's just not a part of vendor workflows; but eventually someone will see the naked emperor and ask why we ignore this data in discovery.

These are examples, and we must recognize that artifacts are different for different operating systems (Windows versus MacOS) and even for different releases of the

^{2.} This GUI access capability was removed in Windows 8 but restored in Windows 10.

same operating system. Artifacts are radically different on phones versus computers. It's complicated, and it changes—frequently.

If you will be using a neutral examiner, draft the protocol to provide for the parties to confer with the examiner so as to establish the scope of work. Too often examiners are saddled with unwieldy protocols poorly tailored to answering the parties' questions because the protocol was drafted without professional guidance.

What you should not expect to occur is your expert gaining direct access to your opponent's digital media. The more likely result is a protocol laying out the steps to be followed by your opponent's expert or by a court-appointed neutral examiner.

§ 22.11 Additional Factors to Consider in Forensic Examination

§ 22.11:1 Establish Who Pays

The cost of a forensic examination can vary widely depending on the nature and complexity of the media under examination, as well as the issues. Forensic examiners usually charge by the hour with rates ranging from approximately \$200 to \$600 per hour depending on experience, training, reputation, and location. Costs of extensive or poorly targeted examinations can quickly run into five and even six figures. Nothing has a greater influence on the cost than the scope of the examination. Focused examinations communicated via clearly expressed protocols tend to keep costs down. Searches should be carefully evaluated to determine if they are over- or underinclusive. The examiner's progress should be followed closely, and the protocol modified as needed. It's prudent to have the examiner report on progress and describe work yet to be done when either hourly or cost benchmarks are reached.

In all events the examination protocol should make clear how, when, and by whom the examiner is compensated for professional time and reimbursed for expenses.

Exemplar Language: Charges for Examiner's professional time and time in transit shall be timely paid by Plaintiffs at the Examiner's customary rates, along with reasonable and customary expenses according to the terms of the rate sheet submitted before appointment. In the event Examiner's charges equal or exceed \$_____, the Examiner shall report progress to the parties and project further charges expected to be incurred to completion.

§ 22.11:2 Address On-Site Acquisition and Supervision

A party whose systems are being acquired and examined may demand to be present throughout the process. This may be feasible while the contents of a computer are being acquired (duplicated); otherwise, it's an unwieldy, unnecessary, and profligate practice. Computer forensic examinations are commonly punctuated by the need to allow data to be processed or searched. Such efforts consume hours, even days, of "machine time," but not examiner time. Examiners sleep, eat, and turn to other cases and projects until the process completes. However, if an examiner must be supervised during machine time operations, the examiner cannot jeopardize another client's expectation of confidentiality by turning to other matters. Thus, the meter runs all the time, without any commensurate benefit to either side except as may flow from the unwarranted inflation of discovery costs.

Demanding that forensically sound acquisition occur on a client's premises versus in an examiner's lab can hugely inflate cost. On-site acquisition may be unavoidable for mission-critical systems like servers, but otherwise I push back against demands to work on a party's premises versus in my own lab. In the lab I can turn to other tasks and stop billing. On-site acquisition and analysis run up the bill unnecessarily and require that I be furnished a workspace that's suitable and secure, perhaps for days or longer.

§ 22.11:3 Recovering Deleted Data

Although the goals of forensic examination vary depending on the circumstances justifying the analysis, a common aim is recovery of deleted data. One court ordered, "if the files . . . have been deleted or altered using a drive-wiping utility, [forensic examiner] will also recover all deleted files and file fragments." *Schreiber v. Schreiber*, 29 Misc. 3d 171, 182, 904 N.Y.S.2d 886, 894 (Sup. Ct. 2010). That's not such a good idea.

Examination protocols shouldn't direct the examiner to, in effect, "undelete all deleted material and produce it." Though that sounds clear, it creates unrealistic expectations and invites excessive cost.

Here's why: A computer manages its hard drive in much the same way that a librarian manages a library. The files are the "books" and their location is tracked by an index. But there are two key differentiators between libraries and computer file systems. Computers employ no Dewey Decimal System, so electronic "books" can be on any shelf. Further, they can be split into chapters, and those chapters stored in multiple

locations across the drive. This is called "fragmentation." Historically libraries tracked books by noting their locations on an index card in a card catalog. Computers similarly employ directories (called "file tables") to track files and fragmented segments of files.

When a user hits Delete in a Windows environment, nothing happens to the actual file targeted for deletion. Instead a change is made to the master file table that keeps track of the file's location. Thus, akin to tearing up a card in the card catalog, the file, like its literary counterpart, is still on the "shelf," but now—without a locator in the file table—the deleted file is a needle in a haystack, buried amidst millions of other unal-located clusters.

Three principal techniques used to recover a deleted file by a computer forensic examiner are detailed in the following three sections.

§ 22.11:4 File Carving by Binary Signature

Because most files begin with a unique digital signature identifying the file type, examiners run software that scans each of the millions of unallocated clusters for file signatures, hoping to find matches. If a matching file signature is found and the original size of the deleted file can be ascertained, the software copies, or "carves out," the deleted file. If the size of the deleted file is unknown, the examiner designates how much data to carve out. The carved data is then assigned a new name and the process continues.

Unfortunately, deleted files may be stored in pieces, as discussed above, so simply carving out contiguous blocks of fragmented data also grabs intervening data having no connection to the deleted file and fails to collect segments for which the directory pointers have been lost. Likewise, when the size of the deleted file isn't known, the size designated for carving may prove too small or large, leaving portions of the original file behind or grabbing unrelated data. Incomplete files and those commingled with unrelated data are generally corrupt and nonfunctional. Their evidentiary value is also compromised.

File signature carving is frustrated when the first few bytes of a deleted file are overwritten by new data. Much of the deleted file may survive, but the data indicating what type of file it was, and thus enabling its recovery, is gone.

File signature carving requires that each unallocated cluster be searched for each of the file types sought to be recovered. When a court directs that an examiner "recover

all deleted files," that's an exercise that could take excessive effort, followed by countless hours spent examining corrupted files. Instead, the protocol should, as feasible, specify the particular file types of interest based on how the machine was used and the facts and issues in the case.

Notably, file carving of deleted information from unallocated clusters is fast becoming untenable by the emergence of solid state and encrypted media. Storage optimization techniques used by solid state drives serve to routinely overwrite oncerecoverable data.

§ 22.11:5 File Carving by Remnant Directory Data

In some file systems, residual file directory information revealing the location of deleted files may be strewn across the drive. Forensic software scans the unallocated clusters in search of these lost directories and uses this data to restore deleted files. Here again, reuse of clusters can corrupt the recovered data. A directive to "undelete everything" gives no guidance to the examiner respecting how to handle files where the metadata is known but the contents are suspect.

§ 22.11:6 Search by Keyword

Where it's known that a deleted file contained certain words or phrases, the remnant data may be found using keyword searching of the unallocated clusters and slack space. Keyword search is a laborious and notoriously inaccurate way to find deleted files, but its use may be warranted when other techniques fail. When keywords are too short or not unique, false positives ("noise hits") are a problem. Examiners must painstakingly look at each hit to assess relevance and then manually carve out responsive data. This process can take days or weeks for a single machine.

§ 22.11:7 Better Practice than "Undelete" Is "Try to Find"

The better practice is to eschew broad directives to "undelete everything" in favor of targeted directives to use reasonable means to identify specified types of deleted files. To illustrate, a court might order, "Examiner should seek to recover any deleted Word, Excel, PowerPoint, and PDF files, as well as to locate potentially relevant deleted files or file fragments in any format containing the terms, 'explosion,' 'ignition,' or 'hazard.'"

§ 22.11:8 Reporting and Deadlines

In the context of digital forensics, "reporting" means many things. As a lawyer–examiner, I create narrative reports setting forth in plain language what I'm seeing in the evidence and what my training and experience suggest it signifies. But most forensic examiners regard reporting as a machine-generated process. It's common for a forensic report to consist of dozens or hundreds of pages of mostly unintelligible gibberish spit out by software. So it's smart to deal with that in the protocol. If the parties need specific questions answered in a narrative fashion, say so. If the analysis must be completed by a time certain, set deadlines for preliminary and final reporting and establish whether meeting those deadlines is feasible for the examiner (recognizing that the examiner has seen no evidence and probably has more questions than answers).

§ 22.11:9 Forensic Acquisition vs. Preservation

Parties and courts are wise to distinguish and apply different standards to requests for forensically sound acquisition versus those seeking forensic examination. Forensically sound acquisition of implicated media guards against spoliation engendered by continued usage of computers and by intentional deletion. It also preserves the ability to later conduct a forensic examination, if warranted.

Forensic examination and analysis of an opponent's ESI is both intrusive and costly, necessitating proof of egregious abuses before allowing one side to directly access the contents of the other side's computers and storage devices (something I caution courts against ordering). By contrast, forensically duplicating and preserving the status quo of electronic evidence costs little and can generally be accomplished without significant inconvenience or intrusion upon privileged or confidential material. Accordingly, courts should freely order forensic preservation on a showing of good cause.

During the conduct of a forensically sound acquisition-

- 1. nothing on the evidence media is altered by the acquisition;
- 2. everything on the evidence media is faithfully acquired; and
- 3. the processes employed are authenticated to confirm success.

These standards cannot be met in every situation—notably in the logical acquisition of a live server or physical acquisition of a phone or tablet device—but parties deviating from a "change nothing" standard should disclose and justify that deviation.

§ 22.12

§ 22.12 Exemplar Acquisition Protocol

An exemplar protocol for acquisition follows, adapted from the court's order in *Xpel Techs. Corp. v. American Filter Film Distributors*, No. SA-08-CV-0175-XR, 2008 WL 744837, at *1 (W.D. Tex. Mar. 17, 2008):

The motion is GRANTED and expedited forensic imaging shall take place as follows:

- A. Computer forensic acquisition will be performed by ______ (the "Examiner").
- B. Examiner's costs shall be borne by the Plaintiff.
- C. Examiner must agree in writing to be bound by the terms of this Order prior to the commencement of the work.
- D. Within two days of this Order or at such other time agreed to by the parties, Defendants shall make the specified computer(s) and other electronic storage devices available to Examiner to enable Examiner to make forensically sound images of those devices, as follows:
 - i. Images of the computer(s) and any other electronic storage devices in Defendants' possession, custody, or control shall be made using hardware and software tools that create a forensically sound, bit-for-bit mirror image of the original hard drives (e.g., EnCase, FTK Imager, X-Ways Forensics, or Linux dd). A bitstream mirror image copy of the media item(s) will be captured and will include all file slack and unallocated space.
 - ii. Examiner should document the make, model, serial, or service tag numbers, peripherals, dates of manufacture, and condition of the systems and media acquired.
 - iii. All images and copies of images shall be authenticated by cryptographic hash value comparison to the original media.
 - iv. The forensic images shall be copied and retained by Examiner in strictest confidence until such time the court or both parties request the destruction of the forensic image files.
 - v. Without altering any data, Examiner should, as feasible, determine and document any deviations of the systems' clock and calendar settings.

- E. Examiner will use best efforts to avoid unnecessarily disrupting the normal activities or business operations of the Defendants while inspecting, copying, and imaging the computers and storage devices.
- F. The Defendants and their officers, employees and agents shall refrain from deleting, relocating, defragmenting, overwriting data on the subject computers or otherwise engaging in any form of activity calculated to impair or defeat forensic acquisition or examination.

§ 22.13 Pulling It Together in Exemplar Protocol

The following exemplar examination protocol was accepted by the Court in a case where the parties sought to determine what a user was doing on a laptop on a single day. As the machine was in a distant state, it was practical that the forensic image be acquired by another examiner and the image shipped to me.

Examination Protocol for Windows Laptop

- I. **Goals:** The purpose of Protocol is to guide Craig Ball, Texas attorney and Certified Computer Forensic Examiner ("Examiner") in identifying and interpreting active and latent artifacts tending to shed light on the nature, extent, and timing of usage, if any, of a Windows laptop machine ("Machine") during specified relevant intervals, as well as in assessing the integrity of the Machine and its contents for data loss, destruction, and alteration during and following the relevant interval (*Date 1*) through (*Date 2*).
- II. **Evidence:** This protocol assumes that Examiner will receive a forensically sound, hash-authenticated bitstream image ("Image") of the Machine's data storage device(s) along with customary chain-of-custody information and baseline data establishing the accuracy or deviation of the Machine's system clock at the time of Image acquisition. Unless otherwise agreed by the parties and the Examiner, only a duly certified Computer Forensic Examiner shall image the Machine and authenticate the chain-of-custody and baseline data.
- III. **Duplication:** The Examiner will make hash-authenticated working and archival copies of the Image. The Image supplied will not otherwise be used for analysis but will be secured until return or disposal.
- IV. **Cooperation and Credentials:** The Parties shall cooperate with the Examiner insofar as promptly supplying nonprivileged information and passwords and credentials required to access and decrypt data on the Image

and accurately interpret the same. No passwords or credentials obtained from the image or furnished by the parties will be used by the Examiner to access data other than found on the Image.

- V. Authorization and Scope: The Examiner may:
 - 1. Load an authenticated working copy of the Image into an analysis platform or platforms and examine the file structures for anomalies.
 - 2. Assess the integrity of the evidence by, for example, checking registry keys to investigate the possibility of drive swapping or fraudulent reimaging and looking at logs to evaluate BIOS clock manipulation. The Examiner may take other reasonable steps to determine if the data supplied is consistent with its stated origins.
 - 3. Look at the various creation dates of key system folders to assess temporal consistency with the machine, OS install, and events.
 - 4. Look for instances of applications employed to alter file metadata or erase/alter usage cache and history data.
 - 5. Note recently installed applications and any antiforensic privacy tools.
 - 6. Refine the volume snapshot to, for example, identify relevant deleted folders, applications and files, orphaned file records, host protected areas, hidden partitions, inter-partition data, and encrypted volumes.
 - 7. Further refine the volume snapshot to unpack compound files (e.g., compressed and container files), compare binary file signatures with file extensions, identify possible encrypted files using entropy testing, hash all files, extract application metadata, and process contents of volume shadow copies.
 - 8. Carve the unallocated clusters for file artifacts using binary signature analysis, seeking deleted files and deleted cache content, temp files, fragments, and system artifacts.
 - 9. Locate and extract registry hives for analysis.
 - 10. Look at the LNK files, index files, TEMP directories, cookies, registry MRUs, shellbags, jump lists, thumbnails, shadow copies, and, as relevant, system and event logs and Windows prefetch area to assess usage of applications, files, and network accesses.

- 11. Generate and export complete file listings with associated file size, file path, and hash and temporal metadata values (other metadata values as relevant and material).
- 12. If indicated, run keyword searches against the contents of all clusters (including unallocated clusters and file slack) seeking relevant data, then review.
- 13. Sort the data chronologically for the relevant Modified Accessed Created (MAC) dates to assess the nature of activity within the relevant interval.
- 14. As feasible, generate a network activity report against, inter alia, index.dat and comparable network activity artifacts to determine, inter alia, if there has been web surfing, web search, e-mail, texting, download or upload activity, or research conducted at pertinent times concerning, for example, how to destroy or alter electronic evidence, conceal system and network usage, and the like.
- 15. Filter for e-mail messaging formats (e.g., PST, OST, NSF, DBX, MSG, and EML), and extract messaging for processing in preferred application. Check OLK folders (Outlook attachment temp storage). Examine container files for relevant e-mail in the relevant interval(s). If webmail, look at cache data. If not found, carve UAC to reconstruct same.
- 16. Identify mobile device (e.g., iTunes, Android) and Cloud (e.g., Drop-Box) synch sources.
- 17. Gather the probative results of the efforts detailed above, assess whether anything else is likely to shed light on the documents and, if not, share conclusions as to what transpired.
- 18. Make recommendations for further lines of inquiry or sources of data, if any.
- VI. **Cost:** Charges for Examiner's professional time and time in transit shall be timely paid by Plaintiffs at the Examiner's customary rates, along with reasonable and customary expenses according to the terms of the Examiner's engagement agreement.

§ 22.14

§ 22.14 Additional Factors to Consider in Drafting Protocols

§ 22.14:1 Privilege and Confidentiality Concerns

The preceding protocol involved a matter where privileged and confidential material and communications weren't a concern, but protocols more typically need to provide for non-waiver of privilege and for counsel's review of the examiner's reporting before it's seen by opposing counsel so that objections can be asserted to disclosure of privileged or protected content. A protocol should also address ex parte communications with the Examiner.

Exemplar Language: To the extent the Examiner has direct or indirect access to information protected by the attorney-client privilege, such access will not result in a waiver of the attorney-client privilege. Unless counsel for all parties are included, there shall be no communications between any party or party's counsel aside from purely ministerial communications necessary to complete the tasks set out in this Protocol.

All data and analyses governed by this Protocol are deemed protected material. Possession of such material is limited to the Examiner the attorneys of record in the captioned cause and their experts. Counsel and their experts may not share or review the protected material in any manner with any other person, including their respective clients.

Any data or reporting resulting from the Examination will be produced by the Examiner to the attorney for the device/media owner for review. No data will be provided to opposing counsel until it has been reviewed and released by the attorney for the device/media owner. A listing of the data that was forwarded to counsel for the device/media owner will be included with the data. This index will include the file name, the date last modified, and the file size, as feasible. Data not in the form of a file will be identified on the listing in a reasonably clear and practical manner. The attorney for the device/media owner will identify on the listing any items that will not be produced and the basis for withholding such items. Items not withheld shall be produced to the party or parties requesting the data along with the listing showing the items withheld and the basis for withholding such items.

Parties may object to withholding of any data, and counsel for the parties shall cooperate on procedures to resolve disputes about withheld data. If the parties cannot resolve a dispute as to the production of withheld data, then any party may move for protection or for an order to compel production.

§ 22.14:2 Forms of Production

The exemplar protocol above doesn't address the challenge of delivering forensic artifacts to counsel in usable formats. Lawyers and courts are conditioned to expect documents and are rarely prepared for data. A crucial forensic artifact may be no more than a few bytes of encoded information bobbing in a sea of unallocated clusters. A handful of these can be converted to a document-like format for review. But what if there are hundreds of thousands of such instances to examine (as commonly occurs when running keyword searches against unallocated clusters)? Lawyers can't expect that the fruits of a forensic examination can be loaded into an e-discovery review platform and treated like documents. Too, lawyers can't expect to load native files into native software applications without altering the evidence. Native applications modify native files.

Skilled forensic examiners are experienced in working with lawyers to facilitate review of forensic artifacts in practical, scalable ways. Since it's not always practical or possible to provide for a form of production in advance of a forensic examination, a protocol should afford the examiner some leeway to supply deliverables in forms suited to assist the parties in their review (and the Court in any *in camera* review).

§ 22.14:3 Ethical Boundaries

Unless the Court expressly permits or the parties agree, a forensic examiner should never use the devices tendered for examination or information derived in the exam to access information beyond that stored on the physical devices and media when tendered for examination. Most examiners know this and will act ethically; however, a thorough protocol should make that restraint clear, so none need worry that an overeager examiner will abuse a booted clone device or a user's login credentials.

Exemplar Language: Examiner shall not use the devices and storage media tendered for examination, or any information or credentials derived from same, to access any electronic information not present on the devices and storage media when tendered for examination. This prohibition includes but is not limited to accessing private online or cloud accounts, email accounts or servers, private social media sites, and banking and credit card accounts and transactions.

§ 22.14:4 Other Points to Ponder

A protocol may need to address topics such as disposition of evidence after analysis, data retention and destruction duties (including financial responsibility for same), amenability to discovery (deposition and subpoena), and applicability of protective orders.

It's useful to empower the examiner to make recommendations for further lines of inquiry or sources of data. Certainly, the parties and the Court must be sensitive to suggestions that smack of make-work; but a skilled, ethical examiner will often have the best ideas where to go to find other relevant electronic evidence.

§ 22.15 Conclusion

Crafting a forensic examination protocol demands more than finding a good form to filch. It requires a clear sense of about what you seek to accomplish through an examination and the ability to express those goals with enough technical specificity to guide a diligent examiner to the artifacts that will answer your questions. There's often a tension between one side's wish to rein the examiner in and the other's to turn the examiner loose. A good protocol balances the two and affords the examiner just enough discretion to follow the electronic evidence and let it tell its tale.

§ 22.16 Frequently Asked Questions

How do I preserve the status quo without requiring a party to stop using its systems? The ongoing use of a computer system erodes the effectiveness of a computer forensic examination and serves as an ongoing opportunity to delete or alter evidence. Where credible allegations suggest the need for forensic examination to arise, the best course is to immediately secure a forensically sound image of the machine or device acquired by a qualified technician and authenticated by hashing. Alternatively the party in control of the machine may agree to replace the hard drive and sequester the original evidence drive so that it will not be altered or damaged.

A party wants to have its technicians make "ghost" images of the drives. Are those forensically sound images? No, only tools and software suited to the task collect every cluster on a drive without altering the evidence. Other software, or the failure to employ write protection hardware devices, will make changes to the evidence and fail to collect data in all of the areas important to a thorough forensic examination. Even the right software and hardware in unskilled hands is no a guarantee of a forensically sound acquisition.

The use of other imaging methods may be entirely sufficient to meet preservation duties when issues requiring computer forensics issues aren't at stake.

Do servers need to be preserved by forensically sound imaging, too? Though forensic examiners may differ on this issue, forensically sound imaging of servers is generally unwarranted because the manner in which servers operate makes them poor candidates for examination of their unallocated clusters. This is an important distinction because the consequences of shutting down a server to facilitate forensic acquisition may have severe business interruption consequences for a party. For preservation in e-discovery, live acquisition of the server's active data areas is usually sufficient and typically doesn't require that the server be downed.

What devices and media should be considered for examination? Though computer forensics is generally associated with servers, desktops, and laptops, these are rarely the only candidates for examination. When they may hold potentially relevant ESI, forensic acquisition and/or examination could encompass external hard drives, thumb drives, tablet devices, smart phones, webmail accounts, cloud storage areas, media cards, entertainment devices with storage capabilities (e.g., iPods and gaming consoles), digital cameras, optical media, legacy media (e.g., floppy and ZIP disks), automobile air bag modules and incident data recorders ("black boxes"), GPS units, backup tapes, and any of a host of others, digital storage devices and Internet of Things sources. Moreover, machines used at home, legacy machines sitting in closets or storage rooms, and machines used by proxies like secretaries, assistants, and family members must be considered as candidates for examination.

How intrusive is a computer forensic examination? A computer forensic examination entails that the devices and media under scrutiny be acquired in a forensically sound manner. This process requires a user to surrender his or her computer(s) for several hours, but rarely longer than overnight. If a user poses no interim risk of wiping the drive or deleting files, acquisition can generally be scheduled so as not to unduly disrupt a user's activities.

A properly conducted acquisition makes no changes to the user's data on the machine, so it can be expected to function exactly as before upon its return. No software, spy-ware, viruses, or any other applications or malware are installed.

The intrusion attendant to forensic examination flows from the fact that such examination lays bare any and all current or prior usage of the machine, including for personal, confidential, and privileged communications; sexual misadventure; financial and medical recordkeeping; storage of proprietary business data; and other sensitive matters. Though it may be possible to avoid intruding on such data within the orderly realm of active data, once deleted, these relevant and irrelevant data cannot easily be segregated or avoided. Accordingly, it's important for the court to either impose strict limits on the use and disclosure of such information by the examiner or require that the examination be conducted by a neutral examiner obliged to protect the legitimate discovery and privacy concerns of both sides.

What does it cost? Though the forensic preservation of a desktop or laptop machine tends to cost no more than a short deposition, the cost of a forensic examination can vary widely depending upon the nature and complexity of the media under examination and the issues. Forensic examiners usually charge by the hour with rates ranging from approximately \$200 to \$500 per hour according to experience, training, reputation, and locale. Costs of extensive or poorly targeted examinations can quickly run into five and even six figures. Nothing has a greater influence on the cost than the scope of the examination. Focused examinations communicated via clearly expressed protocols tend to keep costs down. Keyword searches should be carefully evaluated to determine if they are over- or underinclusive. The examiner's progress should be followed closely and the protocol modified as needed. It's prudent to have the examiner report on progress and describe work yet to be done when either hourly or cost benchmarks are reached.

Chapter 23

Cross-Border Production Issues

Christopher C. Costello and John J. Rosenthal¹

§ 23.1 Introduction

The advance of technology presents significant challenges to lawyers who must identify, preserve, and collect data for use in litigation. Data now migrates across national borders seamlessly—whether through globalization of industry or the increasing use of the cloud for data storage—while companies and individuals face laws, rules, and regulations that restrict their ability to obtain data from outside the United States. A common thread that connects each cross-border issue, particularly from the perspective of the United States, is that not every country shares the same values with respect to access to information during the discovery process. Indeed, most foreign countries disapprove of U.S. litigants' attempts to obtain information from individuals and/or entities located outside the United States. This disapproval occurs for a variety of reasons, including, among others, the perception that U.S. laws and intelligence practices do not properly protect a data subject's privacy rights, and the perceived risk that U.S. discovery could result in the dissemination of a foreign country's state secrets. Moreover, many of these countries have enacted laws and regulations that strictly define how and when data may be transferred outside their borders.

Additionally, foreign laws and regulations pertaining to cross-border transfers are constantly in flux. While a wealth of rules exists, there is a general lack of clarity with respect to how such rules and regulations are, or should be, applied, and few have been tested in a manner that provides practical guidance. In those cases where individuals and/or entities have challenged the ability of U.S. litigants to obtain discovery from foreign entities or individuals, many U.S. courts have required parties to produce the documents even though such actions run the risk of violating the applicable foreign laws. At the same time, foreign countries have been increasingly more assertive in terms of protecting personal data and enforcing rules designed to limit crossborder transfers. For these reasons, cross-border data transfers present significant

^{1.} Christopher C. Costello, CIPP/E, is a Senior E-Discovery Attorney at Winston & Strawn LLP in New York City. John J. Rosenthal is the Chair of the eDiscovery & Information Governance Group at Winston & Strawn LLP and a partner in Washington, D.C.

challenges to litigants responding to requests seeking the production of data from international sources.

Faced with these hurdles, litigants should be aware of both the risks that await the unwary and the mechanisms by which a party can navigate these cross-border issues while still complying with U.S. discovery obligations. This chapter offers practical advice on how best to address cross-border discovery and production issues to avoid facing a choice between Scylla and Charybdis.² Through a combination of education and understanding, many of the problems discussed below can be avoided, or at least minimized.

§ 23.2 Initial Evaluation

The duty to preserve documents and information for purposes of U.S. litigation begins when the company or individual reasonably anticipates litigation. *See, e.g., Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003). See also chapter 1 of this book. In the context of third parties, the duty to respond generally begins once they have been served with a subpoena or other legal process as required by the local procedural rules.³ The sooner the company or individual becomes aware of potential cross-border production issues, the more quickly it can determine how best to respond and to what extent it must produce the requested data or take steps to protect itself from any potential negative effects, both in the United States and abroad.

§ 23.2:1 Personal Jurisdiction

The starting point of any discussion of cross-border discovery is whether the U.S. court has personal jurisdiction over the foreign litigant or individual in possession of the desired documents and information. One of the main questions for jurisdictional purposes is whether the entity from whom the discovery is sought has sufficient contacts with the particular forum as to render it "essentially at home"⁴ (general jurisdiction) or whether the specific circumstances of the case or actions of the foreign entity allow the U.S. court to exercise authority over the foreign entity.⁵ Personal jurisdiction can be found over an entity if it is a party to an existing lawsuit and does not

^{2.} Scylla and Charybdis were mythical sea monsters noted by Homer in *The Odyssey*; one a sixheaded monster on the shore, the other a whirlpool. In such cases, the company or individual faces unappealing and adverse choices, whichever path is chosen.

^{3.} In some instances the duty to preserve can be triggered upon receipt of a document preservation notice sent by one of the parties.

^{4.} See, e.g., Daimler v. Bauman, 134 S. Ct. 746 (2014).

Cross-Border Production Issues

insufficient contacts exist, however, the court has no power over the party from whom the discovery is sought, and the question of whether the court can compel production becomes moot.

§ 23.2:2 The Hague Convention vs. Federal (and State) Rules Governing Discovery

If the forum court has personal jurisdiction over the foreign individual or entity, the court must then analyze whether it should allow discovery to proceed under the auspices of the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Convention)⁶ or under the applicable state or federal rules of civil procedure. This is a fact-intensive inquiry that involves an analysis of international comity and sovereignty (e.g., the impact a decision to allow or limit discovery will have on the interests of all countries implicated by the discovery).

Under either approach, the party from whom the discovery is requested must analyze whether the production of documents and information in the U.S.-based litigation will subject it to civil and criminal penalties in the foreign jurisdiction where the information resides. This often includes a complicated analysis of foreign statutes, regulations, and/or other administrative requirements that the producing party must satisfy before taking action with regard to the data.

The Hague Convention provides a mechanism for transmitting letters of request from one signatory country to another and for using the judicial authorities in the requested country to facilitate the taking of evidence in the other.⁷ Under the Hague Convention, the requesting party must first obtain a letter of request from the court in which the action is pending. The letter of request must include specific information, such as the authority requesting assistance, the names and addresses of parties to the proceedings,

^{5.} Rule 4(k)(2) of the Federal Rules of Civil Procedure; *Merial Ltd. v. Cipla Ltd.*, 681 F.3d 1283, 1294–95 (Fed. Cir. 2012); *United States v. Aluminum Co. of America*, 148 F.2d 416 (2d Cir. 1945) (Hand, J.).

^{6.} *Opened for signature* March 18, 1970, 23 U.S.T. 2555, 847 U.N.T.S. 241. The United States is a signatory to the Hague Convention.

^{7.} Mutual legal assistance treaties (MLATs) are the most commonly used mechanism for crossborder transfers of data between governmental enforcement authorities regarding proceedings involving public or criminal law. MLATs grew out of comity-based system of letters rogatory. MLATs are agreements between two countries for the purpose of gathering and transferring information to assist in the enforcement of criminal laws. The United States has entered into such agreements with over sixty foreign nations. Although they represent a powerful discovery tool for enforcement authorities, MLATs do limit access to and the use of foreign evidence obtained pursuant to a U.S. proceeding.

the nature of the proceedings, and the evidence to be obtained or the judicial act required to be performed. Hague Convention, Art. 3. The letter of request is then transmitted to the central authority of the foreign country, which then executes the requested action to the extent that it does not run afoul of the limitations placed on the foreign judiciary or prejudice the sovereignty or security of the foreign country. Hague Convention, Art. 12. The responding party has the right to resist it, including on the basis that there is an applicable privilege or duty to refuse to give evidence under either the law of the country where the discovery is being sought or the law of the country where the proceeding is being held. Hague Convention, Art. 11.

Although the Hague Convention has the status of an international treaty and thus must be respected in litigation within the United States, the Supreme Court held in Societe Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa, 482 U.S. 522, 539–40 (1987) that the existence of the Hague Convention "did not deprive the District Court of the jurisdiction it otherwise possessed to order a foreign national party before it to produce evidence physically located within a signatory nation." The Supreme Court determined both that the Hague Convention and the Federal Rules of Civil Procedure are separate tools available to the district court, and that there is no bright-line rule requiring the use of one over the other. However, the Supreme Court warned that lower courts supervising pretrial proceedings "should exercise special vigilance to protect foreign litigants from the danger that unnecessary, or unduly burdensome, discovery may place them in a disadvantageous position." Aerospatiale, 482 U.S. at 546. As such, the court cautioned that "[o]bjections to 'abusive' discovery that foreign litigants advance should therefore receive the most careful consideration," and the "demands of comity in suits involving foreign states, either as parties or as sovereigns" with an interest in the litigation should be respected. Aerospatiale, 482 U.S. at 546.

In determining whether to permit or limit discovery, the Supreme Court emphasized that the district court should consider the following factors: (1) the importance to the litigation of the requested documents or information, (2) the degree of specificity of the request, (3) whether the information originated in the United States, (4) the availability of alternative means of securing the information, and (5) the extent to which the failure to comply with the request would harm the interests of the United States, and vice versa. *Aerospatiale*, 482 U.S. at 544 n.28.

Both the United States Court of Appeals for the Fifth Circuit and Texas federal district courts have addressed the issues raised by *Aerospatiale*. In *In re Anschuetz & Co.*, 838 F.2d 1362, 1363–64 (5th Cir. 1988)—a case involving third-party document requests served on a German company—the Fifth Circuit declined to adopt a presumptive rule

that the Hague Convention procedures should be used before a court can turn to the provisions of the Federal Rules of Civil Procedure. The Fifth Circuit, however, made it clear that district courts have "wide discretion [in deciding] between the two sets of discovery rules [Hague Convention and the Federal Rules]" and any determination of whether the Hague Convention proceedings are appropriate should be made only "after 'scrutiny in each case of the particular facts, sovereign interests, and likelihood that resort to these procedures would prove effective." *Anschuetz*, 838 F.2d at 1364 (quoting *Aerospatiale*, 482 U.S. at 544). The Fifth Circuit also noted that district courts should consider that many foreign countries do not subscribe to the open-ended views regarding pretrial discovery inherent in the U.S. system, and that the "purpose of [t]he Hague Convention is to strike a compromise among different systems of laws in order to facilitate the administration of justice without creating unnecessary friction among the foreign entities involved." *Anschuetz*, 838 F.2d at 1364.

More recently, Texas federal courts have held that the requesting party should first attempt to use the Hague Convention proceedings before turning to discovery under the federal rules.⁸ For example, in *Securities & Exchange Commission v. Stanford International Bank Ltd.*, 776 F. Supp. 2d 323, 326 (N.D. Tex. 2011), the Northern District of Texas, Dallas Division, found that discovery pursuant to the Hague Convention was "reasonable under the circumstances" and directed the court-appointed receiver of the estate of R. Allen Stanford to first seek to obtain discovery from Société Généralé Private Banking (Suisse) S.A. (SG Suisse) under the Hague Convention. *Stanford International Bank*, 776 F. Supp. 2d at 326. The receiver could request documents and information under the federal rules only if the attempt to use the Hague Convention procedures "prove[d] unfruitful." *Stanford International Bank*, 776 F. Supp. 2d at 326.

In reaching its conclusion, the court analyzed the receiver's initial discovery requests under the federal rules in light of the five factors noted by the Supreme Court in Aerospatiale, as well as two additional factors that other courts found to be important: (1) the hardship of compliance on the party from whom discovery is sought, and (2) the good faith of the party resisting discovery under the federal rules. *Stanford International Bank*, 776 F. Supp. 2d at 330. After applying these factors, the court found that although "several factors weigh in the Receiver's favor [application of the federal rules], the weightiest factors support SG Suisse [application of the Hague Convention]

^{8.} In addition, in *Triumph Aerostructures LLC v. Comau, Inc.*, No. 3:14-cv-2329-L, 2015 WL 5502625, at *3 (N.D. Tex. Sep. 18, 2015), the district court noted that even though Canada was not a signatory to the Hague Convention, courts faced with requests for letters rogatory under Section 1781 and Federal Rule of Civil Procedure 28(b) "have looked to the comity analysis set out, in the context of a letter of request to a country that is a party to the Hague Evidence Convention."

procedures]." *Stanford International Bank*, 776 F. Supp. 2d at 330. The factor that weighed in favor of applying the Hague Convention, at least in the first instance, was the argument that if SG Suisse were to comply with the discovery request outside the Hague Convention procedures, it could potentially be subject to "criminal, civil, and administrative penalties." *Stanford International Bank*, 776 F. Supp. 2d at 338.⁹

In making this finding, the court noted that "[i]n examining the hardship on the party from whom compliance is sought, courts also look at likelihood that enforcement of the foreign law will be successful." Stanford International Bank, 776 F. Supp. 2d at 339 (quoting Minpeco, S.A., v. Conticommodity Services, Inc., 116 F.R.D. 517, 526 (S.D.N.Y. 1987); Strauss v. Credit Lyonnais, S.A., 242 F.R.D. 199, 224 (E.D.N.Y. 2007)). The court also noted that SG Suisse "present[ed] evidence suggesting that complying with the Receiver's discovery request would subject it to criminal, civil, and administrative penalties," and that SG Suisse's expert specifically pointed to three financial privacy statutes that provide for criminal liability: article 47 of the Swiss Banking Act and articles 271 and 273 of the Swiss Penal Code. Stanford International Bank, 776 F. Supp. 2d at 338. Other Texas federal district courts have conducted similar analyses. See, e.g., Seoul Semiconductor Co. Ltd. v. Nichia Corp., 590 F. Supp. 2d 832, 834-35 (E.D. Tex. 2008) (although the party "resisting discovery bears the burden of showing that the discovery is unwarranted," in cases where burdensome discovery is requested from a French citizen, the burden should be on "the party requesting discovery" and requires a showing of both relevance and lack of hardship); Madden v. Wyeth, No. 03-cv-00167, 2006 WL 7284528, at *2 (N.D. Tex. Jan. 12, 2006) (the party seeking the application of the Hague Convention bears the burden of proof).10

^{9.} The existence of foreign laws regulating a litigant's ability to comply with discovery requests generally militates in favor of finding hardship. *Stanford International Bank*, 776 F. Supp. 2d at 338. However, not all foreign laws are treated equally. "The prospect that the foreign litigant would face criminal penalties rather than civil liabilities weighs in favor of the objecting party." *Stanford International Bank*, 776 F. Supp. 2d at 338 (quoting *Strauss v. Credit Lyonnais, S.A.*, 242 F.R.D. 199, 225 (E.D.N.Y. 2007)).

^{10.} The takeaway from *Seoul Semiconductor* may well be that parties seeking discovery from foreign entities should make their requests as early in the proceeding as possible to allow the court to determine whether it is appropriate to utilize the Hague Convention or federal rules at a time when it may not be clear that there are alternative sources of the same information.

As this area of the law is still evolving,¹¹ litigants should keep abreast of any new developments and should consider how the facts of their case fit within the framework established by *Aerospatiale* and its progeny.

§ 23.2:3 The Federal Rules' Approach to Cross-Border Discovery

In addition to the procedures available under the Hague Convention, requesting parties can seek to obtain documents and information under the Federal Rules of Civil Procedure. For example, rule 26 allows a party to "obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case" Fed. R. Civ. P. 26(b)(1). There is no territorial limitation built into the federal rules, and thus U.S. courts consistently hold that the rules apply to discovery from parties to the U.S. litigation, as well as to discovery sought from third parties, regardless of their country of origin, as long as personal jurisdiction exists. The broader scope of discovery in the United States stands in stark comparison to systems in civil-law countries, where the court is the fact finder and investigators and individuals only have to produce documents that would be admissible at trial.

Despite the broader scope of the federal rules, rule 26(c) permits the court to issue orders limiting the scope of discovery in certain circumstances, including where such orders are necessary to protect from "annoyance, embarrassment, oppression, or undue burden or expense." *See* Fed. R. Civ. P. 26(c)(1). In such instances, the court can, among other things (1) deny discovery into particular matters; (2) specify the terms for the disclosure, including time and place; (3) limit the scope of discovery into certain matters, either entirely or in part; and (4) require that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specific way. Fed. R. Civ. P. 26(c)(1).¹² In addition, parties propounding discovery requests must certify under rule 26(g) that the request is not frivolous, is consistent with existing law, is not interposed for any improper purpose (such as harassment), and does not result in an unreasonable or undue burden. This rule was designed to curtail the overbroad requests that asked for "any and all" documents relating to topics that were defined as broadly as possible. Courts may impose sanctions when parties make the rule 26(g) certification improperly.¹³

^{11.} For example, on January 30, 2020, the United States District Court for the District of New Jersey held that the defendant had to produce names and job titles of likely custodians even though such information is otherwise protected by the EU's General Data Protection Regulation. *In re Mercedes-Benz Emissions Litig.*, Civ. No. 16-cv-881 (KM) (ESK), 2020 U.S. Dist. LEXIS 15967 (D.N.J. Jan. 30, 2020).

^{12.} Rule 26(c)(1)(A)-(H) sets out the list of times and means through which the court can seek to limit discovery.

Companies or individuals facing requests seeking production of documents and information should determine whether to seek the protections of the Hague Convention or those provided by rule 26, or both. In either event, as this area of the law is still evolving, litigants should continue to monitor how U.S. courts approach such decisions and shape their strategies accordingly.

§ 23.3 Laws and Regulations Governing Cross-Border Transfer of Information

To assist the court in resolving discovery disputes involving foreign data, litigants should bring to the court's attention the existence of foreign laws and regulations that prohibit or limit their ability to disclose the requested information. Although these rules and regulations are not always easily categorized, they typically involve data privacy or data protection rules, blocking statues, and state secrets laws.

§ 23.3:1 Data Privacy Regulations

A large number of countries outside the United States have implemented or are in the process of implementing data privacy regulations that prohibit the collection, use, and transfer of personal information across national borders unless certain requirements have been met (e.g., the individual whose data is at issue consents to such transfer, the company completing the transfer has put in place sufficient internal protections to guarantee the safety and security of the data, and the country to which the data is being transferred offers adequate protections). Other exceptions typically apply when the personal data is needed to prosecute or defend legal claims or is otherwise required to be disclosed by law or government action.

The most well-known example of such a privacy regime is that established in the European Union (EU).¹⁴ In 1995, the EU adopted the EU Data Protection Directive, which in Article 1(1) stated that the EU member states agreed to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." Although each of the member coun-

^{13.} See, e.g., Mancia v. Mayflower Textile Services Co., 253 F.R.D. 354 (D. Md. 2008) (containing an in-depth discussion of rule 26(g) and its application to discovery disputes).

^{14.} Regulation (EC) No. 45/2001 of the European Parliament (EU Data Protection Directive). On October 24, 1995, the European Parliament and the Council of the European Union adopted Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "EU Data Protection Directive").

Cross-Border Production Issues

other commentary on data privacy and data protection.

tries adopted national policies pursuant to the EU Data Protection Directive, each country enacted a separate data protection regime. This led to certain country-specific differences, which required companies and their counsel to be aware of the differences and plan accordingly. Moreover, each country had its own data protection authority (DPA) tasked with ensuring compliance with the national programs.¹⁵ In addition to the individual DPAs, the Article 29 Data Protection Working Party (Article 29 Working Party), comprising a representative of the DPA of each EU member country, a representative of the EU, and a representative of the European Commission, served as the advisory body for the EU and published working papers, opinions, and

The EU Data Protection Directive was replaced by the General Data Protection Regulation ("GDPR") in May 2018.¹⁶ The GDPR standardizes the approach of EU countries to data privacy/protection, as it does not require implementing legislation on the national level.¹⁷ It also applies to an EU resident's personal data, irrespective of whether the processing takes place in the EU—at least where goods and services are being offered to EU residents or where the EU residents' activities are being monitored. GDPR, Chapter 1, Article 3. Although an examination of the myriad ways in which the GDPR differs from the EU Data Protection Directive is outside the scope of this chapter, it is worth noting that (1) the GDPR allows for the imposition of significant administrative fines of up to €20 million or four percent (4%) of global annual revenue;¹⁸ (2) may require the appointment of a Data Protection Officer ("DPO");¹⁹ and (3) requires notification of data breaches.²⁰ The European Data Protection Board ("EDPB"), which includes representatives from the data protection authorities of each member state and the European Data Protection Supervisor ("EDPS"), replaced the Article 29 Working Party.²¹ The EDPB can, among other things, adopt general guid-

17. The GDPR does in certain circumstances allow EU member states to impose restrictions beyond those contained in the GDPR.

18. See GDPR Article 83. Please note that violations of Articles 44–49 (addressing cross-border transfers) can result in the maximum administrative fines.

- 19. See GDPR Articles 37-39.
- 20. GDPR Articles 33, 34.

§ 23.3

^{15.} For example, in France the Commission Nationale de l'informatique et des Libertés (the "CNiL") serves as the DPA, while in the United Kingdom it is the Information Commissioner's Office (the "ICO").

^{16.} The full name of the regulation is "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons and with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." The text of the GDPR is available at: http://eur-lex.europa.eu/legal-content/ EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

ance to clarify EU data protection laws and adopt consistency findings in cross-border data protection cases.

Under the GDPR, transfers outside the EU are to be made only if certain requirements are met, including: (1) there has been a determination that the foreign country ensures "an adequate level of protection" (GDPR Article 45(1)); (2) the data controller or processor has "provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available" (Article 46(1)); (3) an appropriate set of binding corporate rules is in place (Article 47); or (4) if one of a number of exceptions, called derogations, applies (Article 49). Currently, the United States has not generally been found to ensure adequate protection, and as such in order to transfer personal data to the U.S., a company must be able to satisfy one of the other requirements. Companies should note that, absent a ruling from the Court of Justice of the European Union ("CJEU") to the contrary, the use of the EU Standard Contractual Clauses complies with the requirements of Article 46.

In addition to the EU, many other countries have implemented data privacy and/or protection laws or regulations, each with their own specific requirements. In a number of instances, the data privacy regulations are contained in a variety of regulations, some of which may not yet have the "force of law." For example, in 2013 China implemented the Guideline for Personal Information Protection within Information System for Public and Commercial Services (the "Privacy Guidelines")²² and the Decision on Strengthening Online Information Protection (the "Decision"), which was effective on December 28, 2012.

Since that time, China has implemented a number of protections, including, among others: (1) the Consumer Rights Protection Law of the People's Republic of China; (2) the Provisions on Telecommunications and Internet User Personal Information Protections; and (3) the new Cybersecurity Law, which took effect on June 1, 2017.²³ Thus, when collecting data in China, a party should note that personal information ("PI") may be collected only if the data subject is notified of the following: (1) pur-

23. An unofficial English translation of the Cybersecurity Law is available here: www. newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoplesrepublic-china/.

^{21.} Information about the EDPB and its mission, as well as EDPB guidance on a variety of issues can be found at: https://edpb.europa.eu/edpb_en.

^{22.} The Privacy Guidelines have not yet been given the force of law, and as such it is uncertain whether the Chinese government will try to use any failure to abide by them as grounds for liability and/ or civil or criminal sanctions. An unofficial English translation of the Privacy Guidelines is available here: www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal -information-security-specification/.

pose of collection; (2) means of collection; (3) scope of use of the PI; (4) protective measures employed; (5) name, address, and contact information for the persons cr entities collecting the data; (6) potential risks involved for the data subject; (7) channels and processes for filing a complaint; and (8), when data needs to be transferred to another organization, the purpose for such transmission, the specific PI transferred and the scope of use, and the name, address and contact information of the recipien. The Privacy Guidelines also prohibit the overseas transfer of PI to an entity absent the data subject's consent, government consent, or other explicit legal or regulatory permission. There is no exception for intracompany transfers.

Although the specific requirements of each data protection regime differs, they generally all define personal information broadly. For example, the GDPR defines personal information to include—

any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity.

GDPR Article 4(1). Many countries, including the EU, take a two-tiered approach to personal data, separately defining a category of "sensitive" personal data that requires even greater protections than those afforded to other types of personal data. The GDPR provides extra protections for "special categories of personal data," which it defines as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of ... data concerning health or sex life." GDPR Article 9. Additionally, China's Privacy Guide-lines define personal information as "computer data that may be processed by an information system, relevant to a certain natural person, and that may be used solely or along with other information to identify such natural person," and define "personal sensitive information" as information that would have an adverse impact on the subject if it is disclosed or altered. Privacy Guidelines, Article 3.2.

§ 23.3:2 Blocking Statutes

In addition to data privacy regimes, certain regions and countries²⁴ impose restrictions through blocking statutes designed to prevent production of documents and information for use in U.S. litigation. Countries enact these statutes for a variety of reasons, most predominantly to protect the foreign country's sovereignty as well as its economic interests. Others were specifically enacted in response to cross-border interference by other states, namely the United States.²⁵ Violations of these statutes can result in both civil and criminal penalties.

The French blocking statute is typical.²⁶ It imposes criminal penalties if certain categories of information are transmitted to the United States, such as documents relating to economic, commercial, industrial, financial, or technical matters, as well as any communication that is capable of harming the sovereignty, security, or essential economic interests of France or contravening public policy, specified by the administrative authorities as necessary.²⁷ Violators of the blocking statute can face up to six months in jail or a fine of €18,000 (€90,000 for legal entities), or both.²⁸

Individuals or entities subject to such blocking statutes should raise their existence and the potential impact on their ability to comply with U.S. discovery requests as early as possible in the U.S. proceeding in order to allow the court to determine whether to use the Hague Convention procedures or to issue a protective order.²⁹ Liti-

29. The decision in *In re Activision Blizzard, Inc.*, 86 A.3d 531 (Del. Ch. 2014) underscores the need to be consistent in one's approach toward a blocking statute. In that case, the Delaware Chancery court found that the fact that one of the defendants had participated in a number of U.S. litigations as a plaintiff and never raised the French blocking statute "undercut its ability to invoke the Blocking Statute, now when the shoe is on the other foot." *Activision Blizzard*, 86 A.3d at 550.

^{24.} These countries include, among others, France, Germany, Switzerland, China, and the Canadian province of Quebec.

^{25.} See Quebec's Business Records Protection Act, 1950 R.S.O., ch. 54 (Can.).

^{26.} Section 1134 of the civil code, section 111-4 of the criminal code, 1 bis of the law no. 68-678, dated July 26, 1968, as amended.

^{27.} Law no. 80-538 of July 16, 1980, Article 4.

^{28.} Law no. 80-538, Article 3. In December 2007 the French Cour de Cassation imposed a criminal fine under the French blocking statute against a French lawyer working with a U.S. firm who attempted to obtain information from a French mutual fund company for use in a pending U.S. litigation. *See In re Advocat "Christopher X,"* Cour de Cassation, Chambre Criminelle [Cass. Crim.], Paris, Dec. 12, 2007, Juris-Data no. 2007-332254. It remains unclear what effect the *In re Christopher X* decision will have on determinations of whether to require resort to the Hague Convention in the first instance when the requested party and information are located in France. *See, e.g., Trueposition, Inc. v. LM Ericsson Telephone Co.*, No. 11-cv-4754, 2012 WL 707012, at *3–4 (E.D. Pa. Mar. 6, 2012) (finding existence of French blocking statute and potential criminal penalties did not require resort to Hague Convention when request was made only for jurisdictional discovery).

Cross-Border Production Issues

gants should also memorialize their attempts to secure authorization from the relevant authorities, including any denials received, to demonstrate that they have been working in good faith to resolve the conflict. This allows the party seeking to avoid the discovery to more persuasively argue that it is not simply interposing the existence of the blocking statute as a means to avoid producing damaging documents or information.

§ 23.3:3 Laws Concerning State Secrets and Sensitive Information

In addition to blocking statutes, a number of countries have enacted laws protecting against the disclosure of material that they deem important to national security interests, such as state secrets. For example, in China, the party from whom information is requested must consider whether responding to a request would violate the Law of the People's Republic of China on Guarding State Secrets ("State Secrets Law"), the Measures for Implementing the Law on the Protection of State Secrets of the People's Republic of China (the "Implementing Measures"), China's State Security Law of the People's Republic of China ("State Security Law"), and the Criminal Law of the People's Republic of China ("Chinese Criminal Law") (collectively, the "State Secrets Laws").³⁰ What constitutes a state secret is broadly defined as matters that relate to the national security and interests as determined under statutory procedures and to which access is limited to a small number of persons for a given period of time. State Secrets Law, Article 2. The Chinese authorities, therefore, can exercise significant discretion to determine what constitutes a state secret. In addition, the Chinese authorities have the ability to retroactively classify material as being subject to state secrets protection. Due to the lack of clarity of Chinese law and the sanctions available to Chinese authorities to punish those that violate the law-including criminal sanctions as well as disbarment or suspension from operating in China-entities should seek counsel regarding whether responding to discovery requests might implicate these laws.

§ 23.4 Cross-Border Discovery Options

To the extent a particular legal matter requires cross-border discovery, there are a number of options a producing party can consider to minimize any conflict between

^{30.} Law of the People's Republic of China on Guarding State Secrets, revised April 29, 2010 (unofficial translation), **www.hrichina.org/content/842**; Measures for Implementing the Law on the Protection of State Secrets of the People's Republic of China (issued in 1990), the State Security Law of the People's Republic of China (effective February 22, 1993) (the "State Security Law"), the Criminal Law of the People's Republic of China (effective October 1, 1997) ("Chinese Criminal Law"), unofficial translations available at: **www.hrichina.org/en**

U.S. discovery obligations and any restrictions or protections imposed by the foreign country.

§ 23.4:1 Cooperation

Many discovery impasses—including disputes regarding the production of data located in foreign jurisdictions—can be resolved informally between the parties. A cooperative approach is regularly championed by The Sedona Conference and many U.S. courts. As noted in The Sedona Conference's International Principles on Discovery, Disclosure & Data Protection in Civil Litigation³¹ (the "International Discovery Principles"):

- (1) ... [C]ourts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.
- (3) Preservation, disclosure, and discovery of Protected Data should be limited in scope to that which is relevant or necessary to support any party's claim or defense
- (4) Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.

The earlier in the case litigants discuss these issues and approaches with each other and the court, if necessary, the more likely it is the litigants can find a mutually agreeable path forward that protects both sides from the pitfalls of foreign discovery, while permitting them to vigorously litigate their positions.

§ 23.4:2 Protective Orders

In situations in which the court determines that resort to the Hague Convention is unnecessary, a litigant can seek to limit cross-border discovery pursuant to the Federal Rules of Civil Procedure as a means of minimizing the risk of violating foreign laws, while still complying with its U.S. discovery obligations. Rule 26(c) permits litigants

^{31.} The Sedona Conference, International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition) (Jan. 2017), https://thesedonaconference.org/publication/International_Litigation_Principles, at 1.

Cross-Border Production Issues

to "move for a protective order" to protect them from "annoyance, embarrassment, oppression, or undue burden or expense." Fed. R. Civ. P. 26(c)(1). In its protective order, the court may prevent the disclosure of the requested material, limit the scope of the inquiry, or require that confidential material or trade secrets be treated in a manner that minimizes disclosure, or otherwise specify the terms of the discovery. *See* Fed. R. Civ. P. 26(c)(1)(A)–(H).

The International Discovery Principles support the use of protective orders and other attempts to limit discovery. They advocate a three-stage approach for avoiding or minimizing the conflicts that may arise when discovery is sought from foreign jurisdictions. First, litigants should consider entering into a stipulated protective order³² to extend special protections to data covered by foreign restrictions. Second, litigants can and should consider a phased approach to discovery, which can be memorialized in a scheduling order issued by the U.S. court. Third, litigants should consider agreeing on a "legitimization plan" that seeks to "maximize compliance with the foreign laws and U.S. discovery obligations." International Principles, at 3.

An appropriate protective order concerning the transfer of foreign data to the U.S. might obviate many of the foreign jurisdiction's objections or reservations. Yet, litigants need to recognize that even a comprehensive protective order issued by a U.S. court may not resolve all conflicts with foreign laws and regulations. The earlier the parties discuss the need for such an order, the more likely it is that they will be able to resolve their differences and be able to educate the court on the need for such an order.

§ 23.4:3 Consent

Consent of the data subject to the use of his or her personal data has long been a cornerstone of foreign data privacy and protection regimes. Under those systems, consent typically should be obtained after providing appropriate notice and before processing begins.³³ The individual collecting the data must disclose the purpose for which the data is being collected, the fact that the data subject may withhold his or her consent, the consequences if consent is withheld, and the other entities that will have access to the personal data in the third country. The GDPR defines the data subject's consent as "any freely given, specific and informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a

^{32.} Annexed as Appendix A to the International Principles is an exemplar of a Stipulated Protective Order Re: Protected Data that can be modified according to the needs of the particular situation.

^{33.} To the extent the nature of the processing changes later, consent should be obtained for the additional processing of personal data.

written statement, including by electronic means, or an oral statement."³⁴ Consent is valid only if the data subject can exercise a real choice and there is no risk of deception, coercion, or negative consequences if the data subject withholds his consent. *See* GDPR, Recital No. 42.

Generally, for consent to be considered effective it must be (1) informed (the person or company consenting must be provided with sufficient information to consider whether they wish the processing to go ahead); (2) specific (the consent must relate to specific data processing activities); (3) overtly signified by the data subject (the data subject must take positive action to show its consent, silence will not generally suffice, and written consent of some kind is preferred); and (4) given freely (it may not be obtained by virtue of duress).³⁵

These factors are not simply window dressing. The Article 29 Working Party explains that for consent to be "informed" it must be based on "an appreciation and understanding of the facts and implications of an action."³⁶ This requires that the individual be given "accurate and full information of all relevant issues," including, among others, the nature of the data being processed, the reason for the processing, the recipients of the data, and an explanation of the data subject's rights (such as the right to withhold consent).³⁷ In addition, for the consent to be valid, it must also be specific (it should refer clearly and precisely to the scope and consequences of the data processing being contemplated). Blanket consents that do not address the specific purpose for which the data is being processed may not be enough to shield the data transfer from scrutiny.³⁸ Moreover, as consent must be freely given, the data subject must be able to withhold consent. This requirement presents significant challenges in the employment context, wherein an employee may have only an illusory choice to withhold consent. The Article 29 Working Party has consistently taken the position that "where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting," any consent obtained from the employee is not "freely given."39 Any decision to obtain consent in the employment context depends on the particular needs of a given matter, but companies should consider the challenges and limitations

- 37. Opinion 15/2011, at 19.
- 38. Opinion 15/2011, at 19.

39. Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of data in the employment context, adopted September 13, 2001, at 23.

^{34.} GDPR, Recital No. 32.

^{35.} See Article 29 Data Protection Working Party, Opinion 15/2011, adopted July 13, 2011, at 12.

^{36.} Opinion 15/2011, at 19.

Cross-Border Production Issues

of such consent and may wish to consult counsel to ensure that they have done everything necessary to comply with the applicable laws and regulations.⁴⁰

Adding to the general uncertainty surrounding the use of consent is the fact that countries have different regimes addressing when and how consent can be obtained from individuals who lack full legal capacity. For example, with respect to children, there is no single framework within which to operate. Applicable local laws and regulations may require obtaining consent from both the child and the child's representative or parent, or only the child if he has reached a certain age. The Article 29 Working Party has noted that the "lack of general rules on [child consent] leads to a fragmented approach" and "legal uncertainty, particularly as far as the way children's consent is obtained."⁴¹

There are, in principle, no limits as to the form of consent. For example, in the EU, the Article 29 Working Party states that "[c]onsent should include any indication of a wish, by which the data subject signifies his agreement."⁴² In addition to "written consent," such as a signature on a piece of paper, the Article 29 Working Party emphasizes that consent can include, among other things, "oral statements to signify agreement," or "behavior from which consent can be reasonably concluded," such as dropping a business card in a bowl or submitting information to a company or organization as part of a request for information.⁴³ Those seeking to use consent as an exception to data privacy regimes are encouraged to seek legal counsel to ensure that it adequately addresses all pertinent issues.⁴⁴

§ 23.4:4 Binding Corporate Rules

In an effort to reduce the need to obtain consent for every data transfer between or among corporate units, affiliates, or third parties acting on the company's behalf, the Article 29 Working Party developed a procedure whereby a company can adopt a set of binding corporate rules (BCRs) to ensure that an intra-organizational personal data

^{40.} Obtaining employee consent can be a time-consuming process, so litigants should make sure to consider whether this option is preferable at the earliest possible stage.

^{41.} Opinion 15/2011, at 28.

^{42.} Opinion 15/2011, at 11.

^{43.} Opinion 15/2011, at 11.

^{44.} The ICO has published general guidance on, among other things, when consent needs to be obtained, what constitutes valid consent, and how a data controller should record and manage consent. The ICO's guidance can be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/.

transfer complies with the EU Data Protection Regime.⁴⁵ BCRs are a series of policies, codes, procedures, and rules that a company adopts to govern the movement of data between and among its subsidiaries. Broadly, BCRs must (1) be binding on all entities of the company, (2) provide for policies and procedures that ensure their effectiveness, (3) include a duty to cooperate with the relevant DPAs, (4) describe the geographic and material scope of the transfers covered by BCRs, (5) provide a description of the mechanisms for recording and approving changes to BCRs, and (6) explain how the entity plans to observe the EU's data protection regime.⁴⁶ In fact, the GDPR expressly states that companies can use BCRs to transfer personal data from the EU to other countries that do not otherwise provide adequate protection. GDPR Articles 46, 47.

The development and implementation of BCRs, however, can be an intrusive and expensive process, in many cases requiring fundamental changes to the entity's data handling processes. For this reason, only 132 companies currently use BCRs.⁴⁷ Those that do are typically large multinational corporations with locations in a variety of foreign jurisdictions that need a way to address the daily operational realities of multinational communication and administration.

Prior to the GDPR, the approval process generally involved four steps: (1) designating the lead DPA, (2) submitting a proposed set of BCRs that fulfill the requirements adopted by the Article 29 Working Party,⁴⁸ (3) circulating the proposed BCRs to the other DPAs in the EU for comments, and (4) after receiving these comments and revising the BCRs accordingly, submitting the final set of BCRs for approval.⁴⁹ Under

^{45.} Representatives of the Article 29 Working Party and representatives of Asia-Pacific Economic Cooperation ("APEC") are exploring whether to allow companies that have EU-focused BCRs to be able to transfer data from APEC countries to the EU. News Release, APEC E-Commerce Steering Group, "Promoting cooperation on data transfer systems between Europe and the Asia-Pacific" (Mar. 6, 2013), www.apec.org/Press/News-Release/2013/0306_data.aspx. This review is ongoing, and as a result, companies wishing to obtain the benefits of BCRs and CBPRs must apply separately for each.

^{46.} A number of Working Party ("WP") papers provide specific guidance regarding the necessary elements and principles to be included in BCRs or implemented in conjunction with them. *See* Article 29 Working Party, WP 74 (discussing primary requirements); *see also* Article 29 Working Party, WP 153, adopted June 24, 2008 (discussing additional elements and principles to be found in BCRs); WP 154, adopted June 24, 2008 (providing a framework for the structure of BCRs).

^{47.} See European Commission, List of companies for which the EU BCR cooperation procedure is closed, http://ec.europa.eu/justice/data-protection/document/international-transfers/binding -corporate-rules/bcr_cooperation/index_en.htm.

^{48.} See Article 29 Working Party, WP 195, adopted June 6, 2012 (providing a standard application form and discussing elements and principles to be found in the Binding Corporate Rules for Data Processors), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion -recommendation/files/2012/wp195_en.pdf. Also see WP 133.

the GDPR, this process has been streamlined to some degree.⁵⁰ A company that wishes to implement BCRs should take steps to ensure that its data processing is in compliance with the GDPR, any other applicable data protection directives and local rules and regulations prior to seeking approval of the BCRs. It should be noted, how-ever, that the while the existence of BCRs does allow a company to transfer personal data to other jurisdictions where the company has affiliates and subsidiaries, assuming that they are covered by the BCRs, BCRs do not allow a company to transfer data to third parties outside the corporate group, for example, to an opposing party in an existing litigation.

§ 23.4:5 Standard Contractual Clauses

As an alternative to the more arduous process of creating and obtaining approval for BCRs, companies seeking to transfer personal information from EU countries can use standardized contractual clauses that ensure an adequate level of protection for data transfers outside the EU.⁵¹ The EU approved these model contract clauses for use in the following circumstances: (1) where the transfer is from a data controller located in the EU to a data controller located outside the EU.⁵² and (2) where the transfer is from a data controller located within the EU to a data processor located outside the EU.⁵³ Moreover, the GDPR specifically refers to the model contractual clauses as an acceptable means of providing appropriate safeguards for the transmission of personal data to third countries. Copies of the approved model contract clauses are annexed as exhibits to the Commission decisions and are included as annexes to this chapter.⁵⁴

51. The EU has adopted model contract clauses governing the transfer of personal data outside its borders. See Article 26(2) of Directive 95/46/EC of the European Parliament and Council.

^{49.} In some EU countries, BCRs do not inherently authorize all data transfers, and certain transfers many still require formal notification to the DPA and, in some cases, further approval. As long as the relevant country from which the data originates accepted the company's BCRs, that country's DPA generally grants any later transfer notifications without further issue.

^{50.} The European Commission has links to a number of the Article 29 Working Party documents that explain the approval process for BCRs and provide guidance on how to structure them. See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en. The GDPR has streamlined the approval process by allowing them to be submitted to the primary DPA and then providing that the BCRs will be evaluated in accordance with the consistency mechanism set forth in Article 63 cf the GDPR.

^{52.} Commission Decision 2004/915/EC, Dec. 27, 2004 (alternative set of standard contractual clauses); Commission Decision 2001/497/EC, June 15, 2001 (original set of standard contractual clauses).

^{53.} Commission Decision 2010/87/EU, Feb. 5, 2010.

The use of these model contract clauses obviates the need to make an independent assessment of the adequacy of the protection afforded the rights of each data subject in connection with a particular transfer. If an individual or entity wishes to use the standard model contracts, the contracts cannot be changed in any way, other than to add another party. The model contract clauses, however, may be incorporated into other contracts or agreements, and additional provisions may be added provided they do not alter the effect of the model clauses. In addition, although parties are free to amend the model contract clauses, doing so removes the presumption of adequate protection. Parties that amend the clauses should be prepared to demonstrate that the amended provisions provide adequate safeguards. To avoid disputes regarding these safeguards, parties should consider submitting their proposed language to the relevant DPA for approval before using the clauses in their contracts.

§ 23.4:6 EU–US Privacy Shield

In addition to protective orders, consent, BCRs, and model contract clauses, the United States and the European Union jointly created an additional mechanism to facilitate individual companies' transfer of personal information from the EU to the United States: the EU–U.S. Privacy Shield.⁵⁵ Companies choosing to participate in the program must comply with the seven Privacy Shield Framework Principles, including, (1) notice of what entity is collecting personal data, why it is being collected, and what use will be made of the data; (2) the fact that the data subject has the right to choose not have his or her personal information disclosed or used for a purpose different from the purpose for which it was originally collected; (3) the fact that data controllers are accountable for onward transfers of personal data; (4) the need to take reasonable and appropriate measures to protect against loss, misuse, and unauthorized access; (5) the need to take reasonable steps to ensure that the processing is limited to

55. Additional information about the EU–US Privacy Shield is available at: www .privacyshield.gov/welcome. A similar program exists between the United States and Switzerland. See www.privacyshield.gov/Swiss-US-Privacy-Shield-FAQs. Please note that the EU–US Privacy Shield was created after the Court Justice for the European Union invalidated the prior US–EU Safe Harbor Program.

^{54.} Please note that the validity of standard contractual clauses is currently being challenged. In 2015, Austrian privacy advocate Maximilian Schrems amended his original complaint to argue that Facebook could not rely on the EU's standard contractual clauses for various reasons. See **www.europe-v-facebook.org/comp_fb_ie.pdf**. Subsequently, the Irish Data Protection Commissioner brought proceedings before the Irish High Court, which referred eleven questions to the Court Justice for the European Union (CJEU) for a preliminary ruling. On December 19, 2019, the CJEU Advocate General issued a non-binding opinion finding that the model contractual clauses are valid, and the Court will issue a decision at a later date. The CJEU is expected to issue its rulings on the preliminary questions in 2020. Companies utilizing the standard contractual clauses should monitor the situation.
Cross-Border Production Issues

§ 23.4

the original purpose and that such data is accurate, complete, and current; (6) the provision of a means by which an individual can access, correct, or amend the personal data being processed; and (7) the creation of robust measures for assuring compliance with the principles, including recourse mechanisms for individuals.⁵⁶ In essence, the Privacy Shield allows U.S. data processors to receive personal information from EU countries as long as the U.S. data processors agree to accept restrictions requiring them to treat the data as if still physically located in the EU and subject to the EU Data Protection regulations.

Participation in the Privacy Shield is voluntary. In order to join, a company needs to self-certify and publicly commit to the Privacy Shield Framework. However, once the commitment is made, it is enforceable by the Federal Trade Commission or the Department of Transportation-depending on which one governs the company's actions. To be assured of Privacy Shield benefits, the organization must self-certify annually to the Department of Commerce in writing that it agrees to adhere to the Privacy Shield's requirements, including the need to create a compliant privacy policy, provide links to the Privacy Shield website, and identify the specific independent recourse mechanism selected (e.g., arbitration). It must also state in its published privacy policy statement that it adheres to the Privacy Shield Principles. If an organization fails to comply with the program, it can be held liable under U.S. federal or state laws prohibiting unfair and deceptive acts, as well as for making false statements to the government.57 If an organization persistently fails to comply-where an entity fails to implement or follow safe harbor requirements to the point it can no longer comply with the safe-harbor framework or where it refuses to comply with a final determination by a regulatory body-it will be removed from the Privacy Shield List, will lose the benefits conferred by the Privacy Shield, and will need to return or delete the personal information it has received under the Privacy Shield.

§ 23.4:7 In-Country Review

The production of documents for use in U.S. litigation involves a number of different stages, including preservation, identification, collection, filtering and culling, analyt-

^{56.} See Privacy Shield Framework: Private Sector Enforcement, available at: www

[.]privacyshield.gov/article?id=Enforcement-of-Privacy-Shield. For instance, the Federal Trade Commission has the power to rectify such misrepresentations by seeking administrative orders and civil penalties of up to \$40,000 per violation or \$40,000 per day for continuing violations. In these cases, the organization must also promptly notify the Department of Commerce of its repeated failures. An entity's failure to uphold the safe harbor requirements while simultaneously publicizing its compliance may be criminally liable under the False Statements Act (18 U.S.C. § 1001).

^{57.} See Privacy Shield Framework: Enforcement of Privacy Shield.

ics, and, ultimately, review of such documents for responsiveness and privilege. To meet the specific requirements of a given jurisdiction, litigants should consider whether some or all of these stages should be conducted in the jurisdiction where the data resides. For instance, where there is a concern that the information sought might implicate privacy or state secrets considerations sufficient to prevent or limit production to the United States, litigants should analyze whether it is preferable to have local reviewers conduct the document review within the foreign jurisdiction in a manner that minimizes the risk of violating the applicable foreign regulations.

Even if a litigant decides to conduct a review outside the country of origin, an initial in-country review may alleviate certain cross-border transfer risks by identifying the types of information likely to be subject to further scrutiny under foreign laws. Law firms and companies alike should consider the need for local counsel to ensure that collection, processing, and review efforts comport with the applicable regulations of the foreign jurisdiction. In addition, finding strategic partners, whether third-party vendors, international law firms, or local law firms, to assist with navigating these considerations is an important part of any plan to conduct cross-border discovery.

§ 23.5 Other Considerations

§ 23.5:1 Cloud Computing

The increasing mobility of cloud service providers presents a particularly challenging issue within the context of cross-border data transfers. Generally, cloud computing consists of a set of technologies that provide for Internet-based use and delivery of IT applications, processing capability, storage, and memory space. In contrast to situations in which the entity producing documents hosts the document on its own systems and behind its own firewall, companies using the cloud generally do not maintain their own data on the company's conventional IT systems. The company, instead, accesses the data remotely through web-based applications. Although theoretically freed from a specific physical location, the information is not freed from cross-border transfer issues. For instance, even though data might reside in the cloud, a cloud provider might, as a practical or legal matter, store that data within a number of foreign countries. In such cases, the laws of those foreign countries may govern the processing of the data within their legal boundaries, even though the cloud is boundless. Depending on how and where an entity stores its data, it should consider whether its storage methodology complies with any applicable data protection and privacy regimes.58

§ 23.5:2 International Privilege Issues

Like most common-law countries, the United States recognizes the existence of the attorney-client privilege. The privilege generally applies when a communication is made to and from a lawyer—either working as in-house counsel for a company or at an outside firm—seeking or conveying legal advice. Under the U.S. system, no distinction is made between the in-house lawyer and outside counsel, as long as the communication is made for purposes of obtaining legal advice. In addition, the United States recognizes the work-product doctrine, which affords protection to documents prepared in connection with litigation, including documents prepared by nonlawyers, as long as they were prepared at the request of a lawyer to assist with the litigation. By contrast, most civil-law countries limit the privileges and protections afforded legal communications and work-product. For example, in France, the law recognizes "professional secrecy" for communications made by the client to a lawyer and communications between lawyers, but excludes in-house counsel for the purpose of this privilege.⁵⁹

U.S. courts differ regarding whether to allow the U.S.-based system of privilege to apply in situations in which the foreign data is not protected by an analogous privilege in the country of origin. For example, in 2M Asset Management, LLC v. Netmass Inc., No. 2:06-CV-215, 2007 WL 666987, at *2–3 (E.D. Tex. Feb. 28, 2007), the Eastern District of Texas addressed this issue, noting that there are two general approaches: (1) the predominant interest test and (2) international comity. Applying both tests to the facts before it, the court found that it would look to German law to determine whether the privilege existed. Compare Astra Aktiebolag v. Andrx Pharmaceuticals, Inc., 208 F.R.D. 92 (S.D.N.Y. 2002) (holding that the U.S. attorney-client privilege applied to documents otherwise not protected by Korean law), with In re Rivastigmine Patent Litigation, 237 F.R.D. 69, 77–78 (S.D.N.Y. 2006) (holding that documents prepared by in-house counsel were discoverable). Because the interplay between U.S. and foreign privilege laws remains largely unsettled, counsel should familiarize them-

^{58.} A heavy burden might be imposed on an entity that stores data in a manner that crosses multiple legal boundaries and, therefore, implicates multiple data privacy and protection regimes. *See* Francoise Gilbert, *Global Privacy and Security Law* ch. 1, § 1.05[B] (2015) (discussing France, Germany, and Italy); Council Directive 94/4 art. 8, 1995 O.J. (L. 281) 31, 50 (EC).

^{59.} Article 66-5 of Law No. 71-1130. ("Ir all areas, whether with regard to advice or in the matter of defense, written opinions sent by a lawyer to his/her client or intended for the latter, correspondence between a client and a lawyer, between a lawyer and other lawyers with the exception, for the latter, of correspondence marked 'official,' meeting notes and generally all documents held in a file are covered by professional secrecy.")

selves with the approaches taken by the country of origin as well as any other countries whose laws can provide a basis for asserting a privilege or other protection.

§ 23.5:3 Data Localization Laws

In addition to data privacy laws and regulations, countries have begun to enact data localization laws, which require that data relating to their citizens be stored on servers maintained within the country's geographic borders.⁶⁰ These laws, which have been imposed either on the national level or in connection with regulations of specific industries present additional challenges to the cross-border flow of data. In addition to Russia, the countries of China, Greece, Indonesia, Kazakhstan, Malaysia, Nigeria, and Vietnam have enacted data localization requirements. Australia, Canada, New Zealand, Turkey, Ukraine, and Venezuela, among other countries, have sector-specific data localization requirements. Companies operating in these jurisdictions should ensure that they do not run afoul of the applicable data localization requirements.

§ 23.6 Practical Steps to Minimize Cross-Border Conflicts Before They Arise

In addition to using the methods of accomplishing data transfers after a request has been made, companies should consider the following strategies to minimize any potential conflicts between local data privacy and/or data protection laws and U.S. discovery obligations:

- 1. Understand the company's data infrastructure and storage locations. This can help the company plan for and respond to requests. The company can consider consolidating these data centers or locating them in jurisdictions with less restrictive data protection regimes.
- 2. Understand the data privacy and protection rules and regulations in the various jurisdictions where the company operates and maintains its data. Being armed with the information on what law, rules, and regulations apply and how they are enforced in the home countries will help the company know what objections to raise when requests or subpoenas come in.

^{60.} Russia's data localization law (Russian Federal Law No. 242-FZ) took effect on September 1, 2015, and requires covered entities that process personal information concerning Russian citizens to use databases that are physically located in Russia. Covered entities are those that physically operate in Russia or own a website that targets Russia.

- 3. Consult with the applicable DPAs or other administrative bodies to open a channel of communication when requests are made. Having an active dialogue with the operative regulatory body will make it easier to obtain the approvals (or denials) necessary to produce data or convey to U.S. courts the reason for a company's failure to comply.
- 4. Implement an aggressive records management program. Volume is the enemy both in terms of cost and in terms of possession of information likely to be subject to restrictions on transfers to the United States. By reducing the overall data retained, there will be less data subject to potential production and less data for the relevant authority to review prior to production. In countries in which restricting the production of state secrets is paramount (such as the People's Republic of China), having a strong classification system is key.
- 5. Strengthen internal privacy protections. The existence of internal company protections for personal information will go a long way toward convincing the relevant DPA that the company maintains an adequate level of protection. A well-developed privacy policy that includes obtaining prospective consent to the use of personal data, data security components, and mechanisms for employees and data subjects to correct personal data or file complaints is helpful. The use of BCRs and/or model contract clauses will also make it easier to obtain approval to transfer data.
- 6. Educate business units regarding U.S. discovery obligations. It is helpful for a company to educate its various business units about U.S. discovery obligations and the need to implement legal holds and suspend automatic deletion policies. Crafting a litigation readiness program to be employed when a company reasonably anticipates litigation will assist in meeting these obligations. Through this process, the company can defensibly determine what documents and information need to be preserved and where they can be preserved without fear of violating data protection laws and regulations.
- 7. Establish relationships with law firms and vendors. Should a request to produce documents in a U.S. litigation arise, a company will benefit from engaging law firms and vendors that understand the challenges inherent in cross-border production and the steps necessary to reduce the company's exposure.

§ 23.7 Checklist for Dealing with Cross-Border Production

The following sections are not intended to be an exclusive listing of all factors and circumstances to be considered by an individual or entity that is facing production of documents in a U.S. proceeding, where the documents and information reside abroad and such production may potentially subject the producing party to civil and criminal penalties.

§ 23.7:1 Jurisdiction

- 1. Is the entity from whom the documents and information are sought subject to personal jurisdiction in the U.S. court where the proceeding is pending? If not, may the entity disregard the request?
- 2. Is the U.S. court where the proceeding is pending the appropriate forum for the action, or should a motion be made to dismiss the action or transfer it to a more appropriate jurisdiction under the doctrine of *forum non conveniens*?
- 3. If the U.S. court has jurisdiction over the party from whom the documents are sought, and the U.S. court is the appropriate forum, then should the court resort to the Hague Convention on the Taking of Evidence Abroad in the first instance? Do the factors enumerated in *Societe Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522 (1987) and its progeny support the application of the Hague Convention Proceedings?
 - a. How important is the requested information to the litigation?
 - b. How specific is the request?
 - c. Did the information originate in the United States?
 - d. Are there alternative means of obtaining the same information?
 - e. To what extent will failing to comply with the request harm U.S. interests, and to what extent will complying with the request harm the interests of the foreign country?
 - f. To what extent will complying with the request impose a hardship on the party from whom discovery is sought?
 - g. Is the party resisting discovery acting in good faith?
- 4. Based on the above, should the party resisting discovery move for a protective order under rule 26(c) of the Federal Rules of Civil Procedure or its

state law equivalents, precluding discovery or limiting it in a meaningful way?

§ 23.7:2 Compliance with Applicable Laws and Regulations

- 1. State Secrets Laws
 - a. Does the jurisdiction in which the documents and information reside have law(s) prohibiting the disclosure of state secrets and confidential economic information?
 - i. If so, have all required steps been taken to obtain approval or denials from the relevant authorities?
 - ii. How long will it take to obtain such determinations?
 - b. Should collection, processing, and review be conducted in the foreign country? By nationals of the foreign country?
 - c. Does the company have a relationship with a third-party vendor or law firm knowledgeable regarding these laws and regulations?
- 2. Data Protection Regimes
 - a. Does the information requested contain personal information, defined broadly?
 - b. If so, is there an applicable data protection or data privacy regime?
 - i. National level policies?
 - ii. Regional or provincial level policies?
 - c. If so, does the regime allow for transfers to the United States?
 - d. What is required in order to satisfy the specific requirements of the data protection regime?
 - i. Is consent required?
 - ii. Is there an exception for use in foreign legal proceedings?
 - iii. In the EU, is the entity a member of the EU-US Privacy Shield?
 - iv. Does the company have BCRs or use the EU model contract clauses?
 - e. Are there rules particular to the national or regional DPA?

§ 23.7

§ 23.7:3 Applicability of Attorney-Client and Other Legal Privileges

- 1. What is the scope of attorney-client privilege, work-product doctrine, and other immunities?
 - a. Does the foreign country recognize a right to legal privilege?
 - b. Is so, what type of documents might be privileged?
 - c. In some foreign countries, legal privileges do not extend to communications between in-house counsel and employees.
- 2. How does compliance with foreign laws and regulations limit access or production?

§ 23.7:4 Cloud Considerations

- 1. Data Storage—does the entity store its data in the cloud? If so, in which jurisdictions are the data stored?
- 2. Access
 - a. Are there any impediments to prevent the entity from obtaining access to its data?
 - b. What contractual provisions exist that govern the use and retrieval of the entity's data?

29.1

Annexes

004	EN	Official Jourr al of the European Union		L 385/7
		ANNEX		
		'SET II		
	Standard contractual cla	nuses for the transfer of personal data from the Commu to controller transfers)	unity to third countries (controller	
		Date transfer agreement		
	between			
			(name)	
			(address and country of establishment)	
		hereinafter "data exporter")		
	and			
			(name)	
			(address and country of establishment)	
		hereinafter "data importer"		
		each a "par-y"; together "the parties".		

Definitions

For the purposes of the clauses:

- (a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);
- (b) "the data exporter" shall mean the controller who transfers the personal data;
- (c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;
- (d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that

- (a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.
- (b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.
- (c) It will provide the data importer, when so recuested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

Essentials of E-Discovery

L 385/78	EN	Official Journal of the European Union	. 29.12.20	0.
	(d) It will respond the data import exporter will sti the data import	to enquiries from data subjects and the authority concerning processing of the ter, unless the parties have agreed that the data importer will so respond, in w ill respond to the extent reasonably possible and with the information reasonab ter is unwilling or unable to respond. Responses will be made within a reaso	e personal data by hich case the data ly available to it if nable time.	
	(e) It will make ava clause III, unles Where informat and of their rig by a decision o subjects have a shall also provi	ilable, upon request, a copy of the clauses to data subjects who are third party is the clauses contain confidential information, in which case it may remove tion is removed, the data exporter shall inform data subjects in writing of the r ht to draw the removal to the attention of the authority. However, the data es of the authority regarding access to the full text of the clauses by data subject greed to respect the confidentiality of the confidential information removed, ide a copy of the clauses to the authority where required.	peneficiaries under such information. eason for removal xporter shall abide ts, as long as data The data exporter	
II.	Obligations of the The data importer	e data importer warrants and undertakes that:		
	(a) It will have in accidental or u provide a level protected.	place appropriate technical and organisational measures to protect the per- nlawful destruction or accidental loss, alteration, unauthorised disclosure or of security appropriate to the risk represented by the processing and the nature	sonal data against access, and which e of the data to be	
	(b) It will have in including proc person acting process the pe persons author	place procedures so that any third party it authorises to have access to essors, will respect and maintain the confidentiality and security of the p under the authority of the data importer, including a data processor, sha rsonal data only on instructions from the data importer. This provision c ised or required by law or regulation to have access to the personal data.	the personal data, ersonal data. Any Il be obligated to does not apply to	
	(c) It has no reaso would have a su data exporter (v such laws.	on to believe, at the time of entering into these clauses, in the existence of a ubstantial adverse effect on the guarantees provided for under these clauses, and which will pass such notification on to the authority where required) if it beco	ny local laws that d it will inform the omes aware of any	
	(d) It will process warranties and	the personal data for purposes described in Annex B, and has the legal aut fulfil the undertakings set out in these clauses.	thority to give the	
	(e) It will identify concerning pro subject and the the data export with the provis	to the data exporter a contact point within its organisation authorised to re- cessing of the personal data, and will cooperate in good faith with the data : authority concerning all such enquiries within a reasonable time. In case of I ter, or if the parties have so agreed, the data importer will assume responsibili sions of clause I(e).	spond to enquiries exporter, the data legal dissolution of lity for compliance	
	(f) At the request of to fulfil its resp	of the data exporter, it will provide the data exporter with evidence of financial ponsibilities under clause III (which may include insurance coverage).	resources sufficient	
	(g) Upon reasonab mentation nee pendent or imj by the data ir reasonable not approval from approval the d	ble request of the data exporter, it will submit its data processing facilities, d ded for processing to reviewing, auditing and/or certifying by the data expopartial inspection agents or auditors, selected by the data exporter and not reas protery to ascertain compliance with the warranties and undertakings in tice and during regular business hours. The request will be subject to any ne a regulatory or supervisory authority within the country of the data importer lata importer will attempt to obtain in a timely fashion.	ata files and docu- orter (or any inde- ionably objected to these clauses, with creastary consent or r, which consent or	

Cross-Border Production Issues

2

Annexes

9.12.2004	EN	Official Journal of the European Union	L 385/79
	(h) It wil	l process the personal data, at its option, in accordance with:	
	(i) t	he data protection laws of the country in which the data exporter is established, or	
	(ii) t t t	he relevant provisions (¹) of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is pased in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data (²), or	
	(iii) t	he data processing principles set forth in Annex A.	
	Ι	Data importer to indicate which option it selects:	
	ŀ	nitials of data importer:;	
	(i) It will Econo	not disclose or transfer the personal data to a third party data controller located outside the European mic Area (EEA) unless it notifies the data exporter about the transfer and	
	(i) t f	he third party data controller processes the personal data in accordance with a Commission decision inding that a third country provides adequate protection, or	
	(ii) ti a	he third party data controller becomes a signatory to these clauses or another data transfer agreement pproved by a competent authority in the EU, or	
	(iii) d ti d	lata subjects have been given the opportunity to object, after having been informed of the purposes of the ransfer, the categories of recipients and the fact that the countries to which data is exported may have ifferent data protection standards, or	
	(iv) w o	with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the nward transfer	
III.	Liability	and third party rights	
	(a) Each J betwee party f it caus export	party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as en the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages ses by any breach of third party rights under these clauses. This does not affect the liability of the data er under its data protection law.	
	(b) The p clause export jurisdi breach enforc period agains failed these	arties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and as $l(b)$, $l(d)$, $l(c)$, $ll(a)$, $ll(c)$, $ll(d)$, $ll(c)$, $ll(d)$, $ll(c)$, $ll(a)$, $ll(c)$,	

 ⁽i) "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).
 (i) However, the provisions of Annex A.5 concerning right: of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Selected.

Essentials of E-Discovery

L 385/80		EN Official Journal of the European Union	29.12.2004
	IV.	Law applicable to the clauses	
		These clauses shall be governed by the law of the country in which the data exporter is estable exception of the laws and regulations relating to processing of the personal data by the data importing $II(h)$, which shall apply only if so selected by the data importer under that clause.	lished, with the rter under clause
	V.	Resolution of disputes with data subjects or the authority	
		(a) In the event of a dispute or claim brought by a data subject or the authority concerning the personal data against either or both of the parties, the parties will inform each other about any claims, and will cooperate with a view to settling them amicably in a timely fashion.	processing of the such disputes or
		(b) The parties agree to respond to any generally available non-binding mediation procedure in subject or by the authority. If they do participate in the proceedings, the parties may elect to (such as by telephone or other electronic means). The parties also agree to consider participat arbitration, mediation or other dispute resolution proceedings developed for data protection or	itiated by a data o do so remotely ing in any other lisputes.
		(c) Each party shall abide by a decision of a competent court of the data exporter's country of est the authority which is final and against which no further appeal is possible.	ablishment or of
	VI.	Termination	
		(a) In the event that the data importer is in breach of its obligations under these clauses, then the d temporarily suspend the transfer of personal data to the data importer until the breach is repaire is terminated.	ata exporter may d or the contract
		(b) In the event that:	
		 (i) the transfer of personal data to the data importer has been temporarily suspended by the longer than one month pursuant to paragraph (a); 	data exporter for
		 (ii) compliance by the data importer with these clauses would put it in breach of its leg obligations in the country of import; 	zal or regulatory
		(iii) the data importer is in substantial or persistent breach of any warranties or undertakings these clauses;	given by it under
		(iv) a final decision against which no further appeal is possible of a competent court of th country of establishment or of the authority rules that there has been a breach of the cla importer or the data exporter; or	e data exporter's auses by the data
		(v) a petition is presented for the administration or winding up of the data importer, whether business capacity, which petition is not dismissed within the applicable period for such applicable law; a winding up order is made; a receiver is appointed over any of its as bankruptcy is appointed, if the data importer is an individual; a company voluntary commenced by it; or any equivalent event in any jurisdiction occurs	in its personal or 1 dismissal under sets; a trustee in 7 arrangement is
		then the data exporter, without prejudice to any other rights which it may have against the da be entitled to terminate these clauses, in which case the authority shall be informed where covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.	ta importer, shall required. In cases

Annexes

29.12.2004 EN

Official Journal of the European Union

L 385/81

- (c) Either party may terminate these clauses if () any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding tex:) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.
- (d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated:

FOR DATA IMPORTER

FOR DATA EXPORTER

.....

Essentials of E-Discovery

5/82	EN Official Journal of the European Union	29.12.2
	ANNEX A	
	DATA PROCESSING PRINCIPLES	
	1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.	
	2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.	
	3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as infor- mation about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.	
	4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.	
	5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectificd, amended, or deleted where it is inaccurate or processed against these principles. If there are compeling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.	
	6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.	
	7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.	
	8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:	
	(a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and	
	(ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.	
	or	
	(b) where otherwise provided by the law of the data exporter	

	Official Journal of the European Union	L 385/8
	ANNEX B	
	DESCRIPTION OF THE TRANSFER	
	(To be completed by the parties)	
Densel		
Data subje	crs	
The person	al data transferred concern the following categories of data subjects:	

Purposes of	of the transfer(s)	
The transfe	r is made for the following purposes:	
Categories	of data	
The person	al data transferred concern the following categories of data:	
Pacinianto		
The person	al data transferred may be disclosed only to the following recipients or categories of recipients:	
	and the second only to the following recipients of categories of recipients.	
Sensitive d	lata (if appropriate)	
The persona	al data transferred concern the following categories of sensitive data:	
•••••		
Data prote	ction registration information of data exporter (where applicable)	
Additional	useful information (storage limits and other relevant information)	
Contact no	unis for data protection enominae	
Contact po	ints for data protection enquiries	
Contact po Data impor	tter Data exporter	

Essentials of E-Discovery

L 385/84 EN

Official Journal of the European Union

29.12.2004

ILLUSTRATIVE COMMERCIAL CLAUSES (OPTIONAL)

Indemnification between the data exporter and data importer:

"The parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of these clauses. Indemnification hereunder is contingent upon (a) the party(ies) to be indemnified (the "indemnified party(ies)") promptly notifying the other party(ies) (the "indemnifying party(ies)") of a claim, (b) the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and (c) the indemnified party(ies) providing reasonable cooperation and assistance to the indemnifying party(ies) in defence of such claim.".

Dispute resolution between the data exporter and data importer (the parties may of course substitute any other alternative dispute resolution or jurisdictional clause):

"In the event of a dispute between the data importer and the data exporter concerning any alleged breach of any provision of these clauses, such dispute shall be finally settled under the rules of arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said rules. The place of arbitration shall be []. The number of arbitrators shall be []."

Allocation of costs:

"Each party shall perform its obligations under these clauses at its own cost."

Extra termination clause:

"In the event of termination of these clauses, the data importer must return all personal data and all copies of the personal data subject to these clauses to the data exporter forthwith or, at the data exporter schoice, will destroy all copies of the same and certify to the data exporter that it has done so, unless the data importer is prevented by its national law or local regulator from destroying or returning all or part of such data, in which event the data will be kept confidential and will not be actively processed for any purpose. The data importer agrees that, if so requested by the data exporter, it will allow the data exporter, or an inspection agent selected by the data exporter and not reasonable volted to by the data importer access to its establishment to verify that this has been done, with reasonable notice and during business hours.":

9/10	EN Official Journal of the European Union	12.2.2010
	ANNEX	
	STANDARD CONTRACTUAL CLAUSES (PROCESSORS)	
	For the purposes of Article 26(2) of Directive 95/46/3C for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection	I
	Name of the data exporting organisation:	
	Address:	
	Tel; e-mail:	
	Other information needed to identify the organisation	
	(the data exporter)	
	And	
	Name of the data importing organisation:	
	Address:	
	Tel; e-mail:	
	Other information needed to identify the organisation:	
	(tre data importer)	
	each a 'pa-ty'; together 'the parties',	
	HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.	
	Clause 1	
	Definitions	
	For the purposes of the Clauses:	
	(a) 'personal data', 'special categories of data', 'proce:s/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council o' 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (!);	

(b) 'the data exporter' means the controller who transfers the personal data;

⁽c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

⁽¹⁾ Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

12.2.2010	EN	Official Journal of the European Union	L 39/11

- (d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

 $1. \qquad \mbox{The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.}$

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has cased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

Cross-Border Production Issues

L 39/12		EN	Official Journal of the European Union	12.2.2010
	(c)	that the data import measures specified in	er will provide sufficient guarantees in respect of the technical and organisational security Appendix 2 to this contract;	
	(d)	that after assessment to protect personal disclosure or access, against all other unla the risks presented by and the cost of their	of the requirements of the applicable data protection law, the security measures are appropriate data against accidental or unlawful destruction or accidental loss, alteration, unauthorised in particular where the processing involves the transmission of data over a network, and wful forms of processing, and that these measures ensure a level of security appropriate to the processing and the nature of the data to be protected having regard to the state of the art implementation;	
	(e)	that it will ensure co	mpliance with the security measures;	
	(f)	that, if the transfer in or as soon as possible protection within the	volves special categories of cata, the data subject has been informed or will be informed before, e after, the transfer that its cata could be transmitted to a third country not providing adequate meaning of Directive 95/45/EC;	
	(g)	to forward any notific 8(3) to the data prot suspension;	cation received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause cction supervisory authority if the data exporter decides to continue the transfer or to lift the	
	(h)	to make available to summary description to be made in accord which case it may re-	the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a of the security measures, as well as a copy of any contract for sub-processing services which has lance with the Clauses, unless the Clauses or the contract contain commercial information, in move such commercial information;	
	(i)	that, in the event of processor providing a data importer under	sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- t least the same level of protection for the personal data and the rights of data subject as the the Clauses; and	
	(j)	that it will ensure con	mpliance with Clause 4(a) to (i).	
			Clause 5	
			Obligations of the data importer (1)	
	The	e data importer agrees	and warrants:	
	(a)	to process the persor Clauses; if it cannot p its inability to comply contract;	hal data only on behalf of the data exporter and in compliance with its instructions and the rovide such compliance for whatever reasons, it agrees to inform promptly the data exporter of , in which case the data exporter is entitled to suspend the transfer of data and/or terminate the	
	(b)	that it has no reason from the data exports which is likely to hav promptly notify the c suspend the transfer of	to believe that the legislation applicable to it prevents it from fulfilling the instructions received er and its obligations under the contract and that in the event of a change in this legislation e a substantial adverse effect on the warranties and obligations provided by the Clauses, it will hange to the data exporter as soon as it is aware, in which case the data exporter is entitled to of data and/or terminate the contract;	
	(c)	that it has implemente the personal data tran	ed the technical and organisational security measures specified in Appendix 2 before processing usferred;	
	(¹)	Mandatory requirements of democratic society on the	of the national legislation applicable to the data importer which do not go beyond what is necessary in a basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary	

(2) Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated processions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which co not go beyond what is necessary in a democratic society are, inter alia, intermationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

12.2.2010	EN	Official Journal of the European Union	L 39/13
	(d) that it will promptly	y notify the data exporter about:	
	(i) any legally bind prohibited, such investigation;	ing request for disclosure of the personal data by a law enforcement authority unless otherwise n as a prohibition under criminal law to preserve the confidentiality of a law enforcement	
	(ii) any accidental o	or unauthorised access; and	
	(iii) any request rec otherwise autho	reived directly from the data subjects without responding to that request, unless it has been prised to do so;	
	 (e) to deal promptly an subject to the transf data transferred; 	d properly with all inquiries from the data exporter relating to its processing of the personal data fer and to abide by the advice of the supervisory authority with regard to the processing of the	
	(f) at the request of the by the Clauses whi members and in por the data exporter, w	e data exporter to submit its data-processing facilities for audit of the processing activities covered ch shall be carried out by the data exporter or an inspection body composed of independen ssession of the required professional qualifications bound by a duty of confidentiality, selected by there applicable, in agreement with the supervisory authority;	l ,
	(g) to make available to unless the Clauses information, with th measures in those c	the data subject upon request a copy of the Clauses, or any existing contract for sub-processing or contract contain commercial information, in which case it may remove such commercia he exception of Appendix 2 which shall be replaced by a summary description of the security ases where the data subject is unable to obtain a copy from the data exporter;	i ,
	(h) that, in the event of consent;	of sub-processing, it has previously informed the data exporter and obtained its prior writter	1
	(i) that the processing	services by the sub-processor will be carried out in accordance with Clause 11;	
	(j) to send promptly a	a copy of any sub-processor agreement it concludes under the Clauses to the data exporter	
		Clause 6	
		Liability	
	1. The parties agree t to in Clause 3 or in Cla for the damage suffered	hat any data subject, who has suffered damage as a result of any breach of the obligations referred use 11 by any party or sub-processor is entitled to receive compensation from the data exporte L	i r
	 If a data subject i exporter, arising out of 3 or in Clause 11, beca the data importer agree unless any successor en law, in which case the 	is not able to bring a claim for compensation in accordance with paragraph 1 against the data a breach by the data importer or his sub-processor of any of their obligations referred to in Claus use the data exporter has factually disappeared or ceased to exist in law or has become insolvent is that the data subject may issue a claim against the data importer as if it were the data exporter tity has assumed the entire legal obligations of the data exporter by contract of by operation of data subject can enforce its rights against such entity.	a e ; ; f
	The data importer may	not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities	
	 If a data subject is 1 and 2, arising out of because both the data e insolvent, the sub-proce- its own processing oper- entity has assumed the which case the data sub- its own processing oper- ties own processing oper- oper- ties own processing oper- ties own processing oper- oper- oper- oper- ties own processing oper- oper- ties own processing oper- oper- ties own processing oper- ties own processing oper- oper- ties own processing oper- ties own processing oper- oper- oper- ties own processing oper- ties own processing oper- ties own processing oper-	a not able to bring a claim against the data exporter or the data importer referred to in paragraph a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 1 xporter and the data importer have factually disappeared or ceased to exist in law or have becom ssor agrees that the data subject may issue a claim against the data sub-processor with regard to rations under the Clauses as if it were the data exporter or the data importer, unless any successo entire legal obligations of the data exporter or data importer by contract or by operation of law, in ject can enforce its rights against such entity. The liability of the sub-processor shall be limited to rations under the Clauses.	S L e D r n D D

EN

Annexes

L 39/14

12.2.2010

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the cata importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exis in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely

⁽¹⁾ This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Essentials of E-Discovery

L 39/15

12.2.2010	EN	Official Journal of the European Union
	 The data exporter a data importer pursuant t exporter's data protection 	shall keep a list of sub-processing agreements concluded under the Clauses and notified by the o Clause 5(j), which shall be updated at least once a year. The list shall be available to the data n supervisory authority.
		Clause 12
	0	bligation after the termination of personal data-processing services
	 The parties agree t sub-processor shall, at th the data exporter or sha legislation imposed upon transferred. In that case transferred and will not 	hat on the termination of the provision of data-processing services, the data importer and the te choice of the data exporter, return all the personal data transferred and the copies thereof to all destroy all the personal data and certify to the data exporter that it has done so, unless in the data importer prevents it from returning or destroying all or part of the personal data , the data importer warrants that it will guarantee the confidentiality of the personal data actively process the personal data transferred anymore.
	2. The data importer authority, it will submit	and the sub-processor warrant that upon request of the data exporter and/or of the supervisory its data-processing facilities for an audit of the measures referred to in paragraph 1.
	On behalf of the data	exporter:
	Name (written out in fu	II):
	Position:	
	Address:	
	induced.	
	Other information neces	sary in order for the contract to be binding (if any):
	\bigcirc	Signature
	(stamp of organisation)	
	On behalf of the data	importer:
	Name (written out in fu	II):
	Position:	
	Address:	
	Other information neces	sary in order for the contract to be binding (if any):
	\bigcirc	Signature
	(stamp of organisation)	
	family of organisation)	

Annexes

)	Official Journal of the European Union	12.2.2010
	Appendix 1	
	to the Standard Contractual Clauses	
	This Appendix forms part of the Clauses and must be completed and signed by the parties	
	The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix	
	Data exporter	
	The data exporter is (please specify briefly your activities relevant to the transfer):	
	Data importer	
	The data importer is (please specify briefly activities relevant to the transfer):	
	The personal data transferred concern the following categories of data subjects (please specify):	
	Categories of data	
	The personal data transferred concern the following categories of data (please specify):	
	Special categories of data (if appropriate) The personal data transferred concern the following special categories of data (please specify):	
	Processing operations	
	The personal data transferred will be subject to the following basic processing activities (please specify):	

Annexes

Essentials of E-Discovery

12.2.2010	EN	Official Journal of the European Union	L 39/17
	DATA EXPORTER		
	Name:		
	Authorised Signature		
	DATA IMPORTER		
	Name:		
	Authorised Signature		

L 39/18	EN	Official Journal of the European Union	12.2.2010		
		Appendix 2			
		to the Stanlard Contractual Clauses			
	This Appendix forms par	t of the Clauses and must be completed and signed by the parties.			
	Description of the tec accordance with Clause	chnical and organisational security measures implemented by the data importer in $s \ 4(d)$ and $5(c)$ (or document/legislation attached):			
			•		
			·		
			•		
		ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)	•		
		Liability			
	The parties agree that if or to the extent to which it i	ne party is held liable for a violation of the clauses committed by the other party, the latter will, is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.			
	Indemnification is conting	gent upon:			
	(a) the data exporter promptly notifying the data importer of a claim; and				
	(b) the data importer bein claim (1).	ng given the possibility to ccoperate with the data exporter in the defence and settlement of the			

(1) Paragraph on liabilities is optional.



Chapter 24

Privacy Issues

David J. Kessler, Sue Ross, and Max Kellogg

§ 24.1 Introduction

The issue of privacy has received significant attention in recent years as sources of personal and private information evolve and become accessible through new media and communication technology. The Texas Supreme Court has held that the Texas Constitution protects personal privacy from unreasonable intrusion. *Texas State Employees Union v. Tex. Dept. of Mental Health & Mental Retardation*, 746 S.W.2d 203, 205 (Tex. 1987). The cases addressing the constitutional right to privacy have involved at least two different kinds of interests: the individual interest in avoiding disclosure of personal matters, and the interest in independence in making certain kinds of important decisions. *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977). The former interest is the topic covered in this chapter as it relates to the discovery of private information in the context of civil litigation. According to one Texas court, this "disclosural privacy" "encompasses the ability of individuals to determine for themselves when, how, and to what extent information about them is communicated to others."¹

This chapter looks at the discovery of information that may be protected by rules or laws related to the privacy of the individual whose information is being requested. The chapter reviews the rules of civil procedure that provide methods to protect private information from discovery. In addition, the chapter provides a review of Texas and federal cases that discuss the factors to consider when seeking protections from discovery in the areas of medical, financial, communication, and other types of information.

^{1.} In re Crestcare Nursing & Rehabilitation Center, 222 S.W.3d 68, 73 (Tex. App.—Tyler 2006, orig. proceeding) (citing Industrial Foundation of the South v. Texas Industrial Accident Board, 540 S.W.2d 668, 679 (Tex. 1976)).

§ 24.2 Federal Rules of Civil Procedure

§ 24.2:1 Fed. R. Civ. P. 26(b)(1)—Duty to Disclose; General Provisions Governing Discovery—Discovery Scope and Limits

As of December 1, 2015, the U.S. modified its federal court rules to clarify that the scope of discovery regarding non-privileged materials must be—

proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.²

Although not specifically directed toward privacy interests, the new proportionality provision is similar to the "minimum necessary" concept in privacy, where only the minimum necessary information required for a permitted purpose is to be disclosed.

§ 24.2:2 Fed. R. Civ. P. 26(c)—Protective Orders

The Federal Rules of Civil Procedure provide that "[t]he court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense."³ Such a protective order is commonly issued by a court as a means to address a party's privacy assertions.⁴ For example, in *Pena v. Canelson Drilling (US), Inc.*, the Western District of Texas granted a protective order limiting the disclosure of personnel files of the plaintiff's former employer, and allowed the defendant to produce redacted files.⁵ Generally, protective orders allow a party to either redact personal information (see section 24.7 of this chapter—Restrictions (Redaction, Protective Orders, Confidentiality Agreements)), or produce the documents under seal. The issuance of a protective order will also ensure that per-

^{2.} Fed. R. Civ. P. 26(b)(1); see In re Bard IVC Filters Prod. Liab. Litig., 317 F.R.D. 562, 564 (D. Ariz. 2016) ("The 2015 amendments also added proportionality as a requirement for permissible discovery. Relevancy alone is no longer sufficient—discovery must also be proportional to the needs of the case.").

^{3.} Fed R. Civ. P. 26(c).

^{4.} *Frazier v. Bed Bath & Beyond, Inc.*, No. 11-MC-80270 RS NC, 2011 WL 5854601, at *2 (N.D. Cal. Nov. 21, 2011) (noting that a protective order is a proper form of protection for an employee having to produce personnel files).

^{5.} No. MO:15-CV-00053-HLH-DC, 2015 WL 12734090, at *2 (W.D. Tex. Sept. 8, 2015).

sonal information is not disclosed or displayed on the court's publicly available docket.

A federal court issuing a protective order based on privacy requires the court to balance the privacy interests in the information asserted by one party with the probative value of that information to the party seeking discovery.⁶ "When the probative value of the information is significant, and the privacy interests in the material can be protected by redaction, there is a presumption in favor of discovery."⁷

§ 24.2:3 Fed. R. Civ. P. 5.2—Privacy Protection for Filings Made with the Court

As of December 1, 2007, the federal court rules were modified to require certain personal information to be redacted in publicly filed court documents. The rule changes affected Federal Rule of Appellate Procedure 25, Federal Rule of Bankruptcy Procedure 9037, the Federal Rule of Civil Procedure 5.2, and the Federal Rules of Criminal Procedure 49.1. Federal Rule of Civil Procedure 5.2 requires four categories of personal information be redacted from public filings, regardless of whether the filings are in paper or electronic format: (1) Social Security numbers and taxpayer ID numbers, except that the last four digits may be included in a public filing; (2) an individual's birth date, but the filing may include an individual's birth year; (3) the name of a minor, but the filing may include the minor's initials; and (4) financial account numbers, but the filing may include the last four digits of the financial account number.

Rule 5.2(a) contains certain exceptions. For example, the redaction requirement does not apply to "the record of an administrative or agency proceeding," or "the official record of a state-court proceeding," or "the record of a court or tribunal, if that record was not subject to the redaction requirement when originally filed."⁸ There are limited exceptions from the redaction requirements for Social Security benefit and immigration cases, where that personal information may be directly relevant to the issues, but which are beyond the scope of this chapter. In addition, rule 5.2 contains two additional broad provisions:

(d) Filings Made Under Seal. The court may order that a filing be made under seal without redaction. The court may later unseal

8. Fed. R. Civ. P. 5.2(a)(2)-(4).

^{6.} Arenson v. Whitehall Convalescent & Nursing Home, Inc., 161 F.R.D. 355, 358 (N.D. III. 1995).

^{7.} Arenson, 161 F.R.D. at 358.

the filing or order the person who made the filing to file a redacted version for the public record.

- (e) For good cause, the court may by order in a case:
 - (1) Require redaction of additional information; or
 - (2) Limit or prohibit a nonparty's remote electronic access to a document filed with the court.⁹

§ 24.3 Texas Rules of Civil Procedure

§ 24.3:1 Tex. R. Civ. P. 21C: Privacy Protection for Filed Documents

Effective as of January 1, 2014, Texas amended its rules of civil procedure to add a rule similar to Federal Rule of Civil Procedure 5.2. The rule defines "sensitive data" as:

- (1) a driver's license number, passport number, social security number, tax identification number, or similar government-issued personal identification number;
- (2) a bank account number, credit card number, or other financial account number; and
- (3) a birth date, home address, and the name of any person who was a minor when the underlying suit was filed.¹⁰

The Texas rule does not contain the exceptions listed in its federal counterpart. The Texas rule prohibits filing any electronic or paper document containing sensitive data with the court unless the sensitive data is redacted or the data is specifically required by statute, court rule, or regulation, or is a will or document filed under seal.¹¹ Sensitive data must be redacted by using an "X" in place of each omitted letter or number or by indicating that the data has been redacted.¹² The filing party must notify the clerk if the document contains sensitive data.¹³ Unlike the permissive standard in the

12. Tex. R. Civ. P. 21c(c).

^{9.} Fed. R. Civ. P. 5.2(d), (e).

^{10.} Tex. R. Civ. P. 21c(a); see In re Srivastava, No. 05-17-00998-CV, 2018 WL 833376 (Tex. App—Dallas, Feb. 12, 2018) (holding that "[a trial] transcript, standing alone, is not currently a document filed with the court for purposes of rule 21c" and therefore would not require redaction of this information).

^{11.} Tex. R. Civ. P. 21c(b).

federal rule, the Texas rule flatly prohibits documents containing sensitive data in violation of this rule from being posted on the Internet.¹⁴ The Texas rule also requires that the filing party retain an unredacted version of the document during the pendency of the case and any related appellate proceedings filed within six months of the date the judgment is signed.¹⁵

Texas also amended Texas Rule of Appellate Procedure 9.9 to contain parallel requirements in civil matters. The Texas Rules of Appellate Procedure for criminal matters (rule 9.10) use the identical definition of "sensitive data" but extends the retention period to three years from the date the judgment is signed.¹⁶ Unlike the rules for civil matters, this rule contains exemptions from the redaction requirements, including the defendant's date of birth and address as well as an arrest or search warrant.¹⁷ In addition, Texas laws require certain materials to be sealed, redacted, or kept confidential, such as personal information about jurors, and this rule expressly prohibits making such information publicly available on the Internet.¹⁸

§ 24.3:2 Protective Orders under Tex. R. Civ. P. 192.6, 76a

In Texas, rule 192.6(b) of the Texas Rules of Civil Procedure allows a party to move for a protective order to prevent the discovery of, among other things, personal information.¹⁹ In appropriate circumstances, the court may simply prohibit the discovery of the personal information, or it may order a party to produce the information in a manner that protects the party in some way (such as through redaction, attorney's eyes only, or in camera review).

A party may also ask the court to seal documents produced in discovery if they contain personal or private information, as long as they meet the requirements of rule

- 13. Tex. R. Civ. P. 21c(d).
- 14. Tex. R. Civ. P. 21c(f).
- 15. Tex. R. Civ. P. 21c(c).
- 16. Tex. R. Civ. P. 9.10(d).
- 17. Tex. R. Civ. P. 9.10(c).
- 18. Tex. R. Civ. P. 9.10(g).

19. Tex. R. Civ. P. 192.6(b) provides: "To protect the movant from undue burden, unnecessary expense, harassment, annoyance, or invasion of personal, constitutional, or property rights, the court may make any order in the interest of justice and may—among other things—order that: (1) the requested discovery not be sought in whole or in part; (2) the extent or subject matter of discovery be limited; (3) the discovery not be undertaken at the time or place specified; (4) the discovery be undertaken only by such method or upon such terms and conditions or at the time and place directed by the court; (5) the results of discovery be sealed or otherwise protected, subject to the provisions of rule 76a."

76a(2).²⁰ "Under rule 76a(2) discovery materials can be considered 'court records' under rule 76a(1) even if not filed with the court."²¹ Courts will "balance the public's interest in open court proceedings against an individual litigant's personal or proprietary interest in privacy" in deciding whether to seal court records.²²

§ 24.4 Protecting Data Throughout Discovery

Instances such as hacking, corporate espionage, and data breaches are dramatically increasing around the world. Thus, producing parties in litigation remain vulnerable to the risk that even if they adequately protect data in their own systems, third parties may steal data from the requesting parties' systems.

Parties and counsel who receive data in litigation have an obligation to take reasonable steps to protect that data.²³ Moreover, "[a] requesting party inherits the data privacy and protection obligations that come with the ESI it receives, including the responsibilities that arise from the loss of that information."²⁴

With such responsibilities, the question is not whether a receiving party has a duty to take reasonable steps to protect data, but what is reasonable and proportionate in the context of the matters. It is recommended that an agreement between both parties be reached with respect to security concerns of data. While a receiving party could attempt to address security concerns unilaterally without reaching an agreement with opposing parties, this is a risky strategy. First, they may not know the value of the data they are receiving and, therefore, not know whether their efforts to secure the data are sufficient. Second, reaching agreements with the opposing party in advance

^{20.} Tex. R. Civ. P. 76a(a) provides: "Court records may not be removed from court files except as permitted by statute or rule. No court order or opinion issued in the adjudication of a case may be sealed. Other court records, as defined in this rule, are presumed to be open to the general public and may be sealed only upon a showing of all of the following: (a) a specific, serious and substantial interest which clearly outweighs: (1) this presumption of openness; (2) any probable adverse effect that sealing will have upon the general public health or safety; (b) no less restrictive means than sealing records will adequately and effectively protect the specific interest asserted."

^{21.} In re Browning-Ferris Industries, Inc., 267 S.W.3d 508, 512 (Tex. App.—Houston [14th Dist.] 2008, orig. proceeding) (court reversed the decision of the trial court and remanded for entry of a sealing order).

^{22.} In re Browning-Ferris, 267 S.W.3d at 512.

^{23.} See The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 19 Sedona Conf. J. 1, 179 (2018); see also William LaRosa, New Legal Problems, Old Legal Solutions: Bailment Theory as a Baseline Data Security Standard of Care Owed to Opponent's Data In E-Discovery, 167 U. Pa. L. Rev. 1, note (2019).

^{24.} The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production at 179, n. 147.

of production provides greater certainty as to what is reasonable and prevents the parties from imposing security standards after the fact. Third and finally, producing parties may not be able to actual produce information without having certain data security and breach notice requirements in place.

Finally, it is not only crucial that a receiving party take reasonable and proportional steps to protect the data that it receives in discovery, but that it promptly notify other parties if that data is lost, stolen or improperly accessed. These requirements should be included in an ESI protocol or protective order so that such obligations are clearly spelled out before any incident occurs.

§ 24.5 Privacy Laws and Regulations That May Affect E-Discovery

The United States does not have a single federal privacy law but instead has enacted various laws that focus on the type of data to be protected. The most comprehensive set of federal requirements relates to medical and health information that is subject to the Health Insurance Portability and Accountability Act of 1996, or HIPAA.²⁵ HIPAA does permit disclosure of medical and health information in response to a discovery request in certain circumstances.²⁶ Other federal laws that may affect disclosure of personal information include the Drivers Privacy Protection Act (state motor vehicle records),²⁷ Electronic Communications Privacy Act (electronic communications, wiretaps, etc.),²⁸ Federal Educational Rights and Privacy Act (student education records),²⁹ and Cable Communications Policy Act (personal data of cable subscribers).³⁰ A detailed discussion of the requirements of these and other federal privacy laws is beyond the scope of this chapter.

Some state privacy laws coming into effect may affect e-discovery, yet the extent of their effect is unknown. California became the first state to sign a new law, the California Consumer Protection Act ("CCPA"), effective January 1, 2020, provides consumers with various rights including: knowing what personal information a business collects about them,³¹ allowing consumers to access their personal information a busi-

- 28. 18 U.S.C. §§ 2510-3127.
- 29. 20 U.S.C. § 1232.
- 30. 47 U.S.C. § 551.
- 31. Cal. Civ. Code § 1798.100.

^{25. 42} U.S.C. § 1320d as amended; 45 C.F.R. § 160-164.

^{26. 45} C.F.R. § 512(e) (disclosures for judicial and administrative proceedings).

^{27. 18} U.S.C. §§ 2721–2725.

ness collects on them,³² and importantly granting consumers the right to request that such data be deleted.³³

With respect to the deletion of data, the CCPA states an exception that a business "shall not be required" to comply with the request to delete to "comply with a legal obligation."³⁴ In addition, the CCPA explicitly states that "[t]he obligations imposed on businesses [under the CCPA] shall not restrict a business's ability to: (1) comply with federal, state, or local laws [or] (2) comply with a civil, criminal, or regulatory inquiry, investigation or subpoena or summons by federal, state, or local authorities³⁵ Thus, a legal obligation to preserve data for a pending or reasonably anticipated litigation would prevent a business from deleting the personal information of a consumer.

Further discussion of state privacy laws is beyond the scope of this chapter, but it should be noted that other states are starting to follow California's footprint, including Texas.³⁶

§ 24.6 Cases in Texas Relating to Discovery and Privacy Issues

§ 24.6:1 Medical

Texas case law has attempted to balance the privacy rules promulgated under evidentiary rules, HIPAA, confidentiality statutes, public information laws, and commonlaw principles in various cases. Generally, the courts have been loath to hold that HIPAA preempts Texas state law, often finding harmony between the two. There has been some conflict over whether redaction of personally identifiable information is an adequate measure to protect patient confidentiality. Texas's Public Information Act has also been instrumental in defining the contours of confidentiality in the medical arena.

Under the Texas Rules of Evidence, confidential communications, including personal medical information, between a patient and physician are generally considered privi-

- 34. Cal. Civ. Code § 1798.105(d)(8).
- 35. Cal. Civ. Code § 1798. 145(a).

36. The Texas legislature has introduced two new privacy bills for consideration. One of them, the H.B. 4518, heavily mirrors the CCPA, and also includes the right to request personal information be deleted. Nevada has also passed recent privacy legislation, which took effect in October 2019.

^{32.} Cal. Civ. Code § 1798.100.

^{33.} Cal. Civ. Code § 1798.105.

Privacy Issues

leged and are subject to protections from disclosure.³⁷ Texas courts may, however, rely on certain exemptions in the Texas Rules of Evidence to permit discovery. For example, rule 509(e)(4) exempts from privilege any "communication or record relevant to an issue of the physical, mental, or emotional condition of a patient in any proceeding in which any party relies upon the condition as a part of the party's claim or defense." Tex. R. Evid. 509(e)(4). This exemption may even reach the records of third parties. In the case of In re Christus Health Southeast Texas,³⁸ the plaintiff sought discovery of redacted hospital records detailing emergency room visits of nonparties on the same day the plaintiff was treated. The hospital objected on the grounds of "Physician/Patient privilege, hospital patient privilege, HIPAA privilege."39 The court noted that only a patient, his representative, or the physician may assert the physicianpatient privilege, not a hospital. However, the plaintiff had neither requested nor obtained the consent of any nonparties to disclose the information. The court therefore remanded the decision to the trial court to determine whether the nonparty "patients" conditions are a part of [the plaintiff's] claim rather than simply relevant to the case."40 Moreover, the court cautioned the trial court to ensure that any discovery of nonparty information was "no broader than necessary, considering the competing interests at stake."41

In contrast, in a slip and fall case involving a grocery store, the Corpus Christi Court of Appeals found that disclosure of two incident reports involving customers experiencing similar incidents at the store must be provided to the plaintiff despite the grocery store's claim of invasion of privacy of the customers' data.⁴² The reports contained the customers' names, addresses, day and evening phone numbers, dates of birth, brief descriptions of the incident, and brief summaries of the injuries sustained. The appeals court reasoned that the information "might, under some circumstances, be included within the protected zone of privacy, this is not such a case" due to the limited disclosure. Furthermore, the court found, even if the information were within the zone of privacy, the grocery store failed to meet its burden of proof to establish the privilege and the grocery store had not shown any evidence of a "particular, articulated and demonstrable injury" that would result from disclosure.

42. In re H.E.B. Grocery Co., L.P., No 13-14-00023-CV, 2014 WL 700749 (Tex. App.—Corpus Christi–Edinburg Feb. 18, 2014).

^{37.} Tex. R. Evid. 509(c).

^{38. 167} S.W.3d 596, 597 (Tex. App.-Beaumont 2005, orig. proceeding).

^{39.} In re Christus, 167 S.W.3d at 598.

^{40.} In re Christus, 167 S.W.3d at 602.

^{41.} In re Christus, 167 S.W.3d at 603 (quoting R.K. v. Ramirez, 887 S.W.2d 836, 843 (Tex. 1994)).

Under section 74.052 of the Texas Civil Practices and Remedies Code, a plaintiff in a medical malpractice claim must provide the defendant with a written form authorizing the release of healthcare information from nonparty medical providers. *See* Tex. Civ. Prac. & Rem. Code § 74.052. The Texas Supreme Court held that the clear language of section 74.052 authorizes ex parte contacts between defense attorneys and the non-party medical providers, rejecting the plaintiff's demand for a protective order and the argument that section 74.052 does not contemplate ex parte contacts and that HIPAA privacy rules preempt section 74.052 and forbid such contacts.⁴³ The court held that HIPAA itself allows the disclosure of protected health information if the patient has executed a valid, written authorization."⁴⁴

In a health-care liability wrongful death case where the defending physician took his own life a month after the patient died, the patient's estate claimed that the physician's "surgical, medical, physical, mental, emotional, and psychological abilities" were a contributing cause to the patient's death. The plaintiffs sought discovery of medical and psychological records pertaining to his medical and psychological conditions for ten years prior to his death. The trial judge ordered redaction of certain portions of the records but ordered production of the remainder. The appellate court agreed with the trial judge's approach:⁴⁵

First, he ordered a limited production of records for *in camera* review, narrowly tailoring the production of evidence, by balancing the need for the production of relevant information with the interest or producing the minimum possible violation of Dr. Hodges's privilege. He accomplished this by (1) limiting the time period of the records to be produced to ten years, (2) barring Real Parties in Interest from deposing Dr. Hodges's widow (in deference to the traumatic nature of his suicide), and (3) prohibiting Real Parties in Interest from obtaining the identity of Dr. Hodges's medical and mental health provider. Judge Board then conducted an *in camera* review of the records produced and further limited the production of evidence by specifically identifying portions that were to be redacted before the remaining portion was produced.

In re McAdams, at *4.

^{43.} In re Collins, 286 S.W.3d 911 (Tex. 2009 (orig. proceeding)).

^{44.} In re Collins, 286 S.W.3d at 916.

^{45.} In re McAdams, No. 07-18-00345-CV, 2018 WL 5573786 (Tex. App.—Amarillo, Oct. 29, 2018).
Privacy Issues

Although HIPAA protects medical records by requiring certain procedures and consent forms before they can be disclosed, the results of blood tests taken during medical examinations may be exempt when used by law enforcement to show blood alcohol content. Upholding precedent prior to the enactment of HIPAA,⁴⁶ the Waco court of appeals held that the defendant had no standing to challenge the state's use of blood-alcohol test results obtained during the course of treatment of injuries sustained in a car accident, despite the fact that the state originally obtained those results via a "sham" subpoena.⁴⁷ While recognizing that "there is no Fourth Amendment reasonable expectation of privacy protecting such blood-alcohol test results," the court recognized that the state did violate HIPAA by obtaining the remainder of defendant's medical records under the sham subpoena.⁴⁸

On the other hand, there were violations when the state obtained a blood sample that was drawn by medical personnel from an individual involved in a traffic accident, but the medical personnel never analyzed the sample.⁴⁹ The state's analysis constituted a "search" requiring a warrant and therefore violated both the U.S. and Texas Constitutions.

The Houston court of appeals has ruled that two lawyers could not be held liable for invasion of privacy for allegedly obtaining the plaintiff's medical information from another lawyer in an unrelated case.⁵⁰ The court relied on Texas case law holding that "attorneys should not be held liable for statements or actions taken in the course of representing their clients" absent fraudulent or malicious conduct and that "an invasion-of-privacy claim is not one of the recognized types of behavior that falls into the category of fraudulent or malicious conduct."⁵¹

51. Sacks, 401 S.W.3d at 342.

^{46.} State v. Hardy, 963 S.W.2d 516, 527 (Tex. Crim. App. 1997) (holding that there is no Fourth Amendment reasonable expectation of privacy protecting blood alcohol results from tests taken by hospital personnel solely for medical purposes after *ε* traffic accident).

^{47.} State v. Jewell, No. 10-11-00166-CR, 2013 WL 387800 (Tex. App.—Waco Jan. 31, 2013, no pet.) (mem. op., not designated for publication). See also State v. Huse, 491 S.W.3d 833 (Tex. Crim. App. 2016), cert. denied, 137. S. Ct. 1066 (2017) ("We have no doubt that HIPAA might support a broader claim that society now recognizes (if it did not already) that a patient has a legitimate expectation of privacy in his medical records in general. . . . HIPAA nonetheless provides specific exceptions" including grand jury subpoenas, which were used in the blood-alcohol records case.)

^{48.} Jewell, 2013 WL 387800, at *5. The court permitted the use of the medical records once the state cured the subpoena.

^{49.} State v. Martinez, 534 S.W.3d 97, 101-2 (Tex. App. 2017), aff'd, 570 S.W.3d 278 (Tex. Crim. App. 2019).

^{50.} Sacks v. Zimmerman, 401 S.W.3d 336 (Tex. App.-Houston [14th Dist.] 2013, pet. denied).

§ 24.6:2 Public Information Act

In *Abbott v. Texas Dept. of Mental Health & Mental Retardation*,⁵² the Austin court of appeals held that Texas's Public Information Act ("PIA")⁵³ qualifies as one of the exemptions to the privacy rule promulgated under HIPAA section 164.512(a), thus compelling the Texas Department of Mental Health and Mental Retardation to release statistical information pertaining to abuse as well as the names of facilities investigated. In a complex analysis balancing the PIA with the privacy rule, the court concluded that when a request for protected health information is made under the PIA, an exception to nondisclosure found in the HIPAA regulations applies.⁵⁴ It is then incumbent on the agency to determine whether the PIA compels or is subject to exemption from disclosure, as when information is deemed "confidential" under a judicial decision or statute.⁵⁵ The court concluded that "the information requested in this case [was] not confidential and [was], therefore, subject to release under the Public Information Act."⁵⁶

Construing the PIA in light of the Texas Occupations Code,⁵⁷ the Austin court of appeals in *Texas State Board of Chiropractic Examiners v. Abbott* held that the board's files pertaining to complaints against a chiropractor were exempt from disclosure to a requestor.⁵⁸ Under the Code, the board's investigation files are deemed confidential and, thus, presumably exempted from disclosure under the PIA.⁵⁹ However, the Code also gives a requestor the right to compel disclosure of their own medical records.⁶⁰ In reconciling this conflict, the court found that the two Code provisions

- 52. 212 S.W.3d 648 (Tex. App.—Austin 2006, no pet.).
- 53. Tex. Gov't Code §§ 552.001-.353.
- 54. Abbott, 212 S.W.3d at 662.
- 55. Abbott, 212 S.W.3d at 662.

56. Abbott, 212 S.W.3d at 665. See also Paxton v. City of Dallas, No. 06-18-00095-CV, 2019 WL 2119644 (Tex. App—Texarkana May 15, 2019) (the privilege for noncore work product makes information confidential for PIA purposes); Paxton v. Texas Health & Human Servs. Comm'n, 550 S.W.3d 207, 213 (Tex. App—Austin 2017, pet. denied) (information regarding healthcare service providers; Medicaid claims for reimbursement is subject to PIA disclosure, excluding information identifying individuals, information disclosing individuals' personal information, or information permitting someone to derive such information); Paxton v. City of Liberty, No. 13-13-00614-CV, 2015 WL 832087 (Tex. App.—Corpus Christi–Edinburg Feb. 26, 2015) (disclosure required for city records of a specific personal phone number that belonged to a police officer but was used in official business. Phone records relating to officer's personal information and did not need to be disclosed).

- 57. Tex. Occ. Code §§ 201.205, 201.206, 201.404, 201.405.
- 58. 391 S.W.3d 343 (Tex. App.—Austin 2013, no pet.).
- 59. Abbott, 391 S.W.3d at 346.
- 60. Abbott, 391 S.W.3d at 346.

Privacy Issues

were enacted for different purposes and that the board's investigation files were privileged from disclosure under the PIA "[b]ecause the privilege asserted by the Board here is one intended to protect the integrity of the Board's regulatory process, rather than the requestor's privacy interests."⁶¹

§ 24.6:3 Financial Information

By and large, Texas allows for moderate discovery of financial information. Tax returns of litigants are generally discoverable where relevant. Similarly, evidence of a defendant's net worth is discoverable where punitive or exemplary damages are at issue, although as of September 1, 2015, Texas enacted a new law that changes the way net-worth discovery will be conducted for exemplary damages claims. However, Texas courts have recognized that due to "privacy interests inherent in" income tax returns, such returns are not discoverable as evidence of net worth if there are other adequate methods to obtain the necessary net worth information.⁶² Additionally, the courts will not permit overly broad requests of financial information, such as credit applications or loan requests that appear to be duplicative or merely intended to harass.

With respect to discovery of evidence of net worth for exemplary damages claims, the 2015 law, Texas Civil Practice and Remedies Code section 41.0115(a), states:

On the motion of a party after notice and hearing, a trial court may authorize discovery of evidence of a defendant's net worth if the court finds in a written order that the claimant has demonstrated a substantial likelihood of success on the merits of a claim for exemplary damages.

The new law specifically permits evidence submitted in support of or in opposition to a motion made under this subsection to be in the form of an affidavit or a response to discovery. If the trial court authorizes the discovery, then the law requires that the court order "may only authorize use of the least burdensome method available to obtain the net worth evidence."⁶³ Note that the burden of proof with respect to tax returns and related information (such as 1099s) originally lies with the party seeking to prevent production, but once the resisting party objects, the burden shifts to the

^{61.} Abbott, 391 S.W.3d at 351.

^{62.} In re Vaughan, No. 13-18-00541-CV, 2019 WL 962381, at *5 (Tex. App. Feb. 27, 2019) (finding that while plaintiff showed that defendant's tax returns were relevant, plaintiff failed to argue or show that information sought could not be found by less intrusive means other than getting tax returns).

^{63.} Tex. Civ. Prac. & Rem. Code § 41.0115(b).

party seeking to obtain the documents to show that the tax returns and related documents are both relevant and material to the issues and cannot be discovered through other "less intrusive means."⁶⁴

In a case arising under the Fair Labor Standards Act, both plaintiffs and defendant requested discovery of financial information.⁶⁵ The United States District Court for the Western District of Texas held that, where the plaintiffs' status as employees or contractors was at issue, their tax returns were relevant and discoverable.⁶⁶ Similarly, the court held that the defendant's tax returns were also relevant and discoverable as they tended to show how the defendant classified the plaintiffs' work and no other documents were duplicative.⁶⁷ However, the court denied the defendant's request for other financial records, such as the plaintiffs' loan applications, credit card statements and bank records, on the grounds that such requests were "invasive and intrusive, subjecting Plaintiffs to a very substantial burden."⁶⁸

In a personal injury case premised on negligence and premises liability, the plaintiff sought (1) deposition of the defendant's accountant, (2) tax returns for the defendant and the multiple businesses he conducted from the premises, and (3) information reflecting the defendant's net worth.⁶⁹ The Corpus Christi court of appeals overruled the defendant's objections, first finding that there is no accountant-client privilege despite section 901.457 of the Texas Occupations Code, which protects the confidentiality of accountant-client communications, and that, even if there were a privilege, the defendant failed to adequately plead such a relationship.⁷⁰ Second, the court held that the tax returns of the defendant's nonparty businesses were discoverable to the extent that they were relevant to show the defendant's control of the premises.⁷¹ Last, the court held that evidence of the defendant's current net worth was discoverable, as punitive damages were being sought, but evidence of the defendant's past net worth was deemed irrelevant and undiscoverable.⁷²

- 67. Rafeedie, 2011 WL 5352826, at *4.
- 68. Rafeedie, 2011 WL 5352826, at *3.

69. In re Arnold, No. 13-12-00619-CV, 2012 WL 6085320 (Tex. App.—Corpus Christi–Edinburg Nov. 30, 2012, orig. proceeding) (mem. op.).

- 70. In re Arnold, 2012 WL 6085320 at *3-4.
- 71. In re Arnold, 2012 WL 6085320 at *5.
- 72. In re Arnold, 2012 WL 6085320 at *6-7.

^{64.} In re Vaughan, No. 13-18-00541-CV (Tex. App.—Corpus Christi-Edinburg Feb. 27, 2019) (2019 WL 962381).

^{65.} Rafeedie v. L.L.C., Inc., No. A-10-CA-743 LY, 2011 WL 5352826 (W.D. Tex. Nov. 7, 2011).

^{66.} Rafeedie, 2011 WL 5352826, at *2.

§ 24.6:4 Social Media

Although social media frequently is intended to be readable by the public, most social media sites permit users to limit access through various privacy settings. Similar to courts around the country, Texas courts are beginning to face the privacy issues raised by social media. For example, in 2013 the Beaumont court of appeals ruled in a health-care liability case in which the hospital sought copies of the plaintiffs' postings on any social media sites.⁷³ The plaintiffs claimed that the request was an invasion of their privacy and that the request was a "fishing expedition."⁷⁴ The trial court denied the hospital's request, and the appellate court affirmed on narrow grounds that "the Lowes did not establish that they had an expectation of privacy in their statements on social media sites. Nevertheless, a request without a time limit for posts is overly broad on its face."⁷⁵

Cases are mixed at the federal level with respect to data where the social media user has used a privacy setting to render the information not generally public. Two federal district court cases from 2010 illustrate the contrasting views. The court in the Central District of California found social media site information similar to employment and bank records for purposes of standing⁷⁶ and found that those records that "are not readily accessible to the general public" may be beyond the reach of a subpoena.⁷⁷ In contrast, a court in the Southern District of Indiana ruled that "a person's expectations and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery" and stated that a protective order may address the issue.⁷⁸

§ 24.6:5 Hard Drives

The Texas courts have addressed whether parties may obtain discovery of hard drive media from their adversaries in the course of a civil litigation. Hard drives can poten-

^{73.} In re Christus Health Southeast Texas, 399 S.W.3d 343, 347–48 (Tex. App.—Beaumont 2013, no pet.).

^{74.} In re Christus, 399 S.W.3d at 348.

^{75.} In re Christus, 399 S.W.3d at 348.

^{76.} Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 974 (C.D. Cal. 2010) ("[A]n individual has a personal right in information in his or her profile and inbox on a social networking site and his or her webmail inbox in the same way that an individual has a personal right in employment and bank records.").

^{77.} *Crispin*, 717 F. Supp. 2d at 991 ("With respect to webmail and private messaging, the court is satisfied that those forms of communications media are inherently private such that stored messages are not readily accessible to the general public.").

tially contain very large amounts of information, including personal or private information that is not relevant to the matter. Texas courts have therefore recognized that litigants must meet certain standards before they will be allowed to obtain access to the drives.

The Texas Supreme Court addressed this issue in the case of *In re Weekley Homes*, *L.P.*, 295 S.W.3d 309 (Tex. 2009) (orig. proceeding). Weekley Homes brought a mandamus action to review the trial court's order that it produce the hard drives of several of its employees. The supreme court defined a number of threshold factors that must be met before allowing such an order, noting "the highly intrusive nature of computer storage search and the sensitivity of the subject matter."⁷⁹ It stated further that if a party makes a threshold showing to permit access to hard drives, "[c]ourts must also address privilege, privacy, and confidentiality concerns."⁸⁰

In the case of *In re Pinnacle Engineering, Inc.*, 405 S.W.3d 835, 846 (Tex. App.— Houston [1st Dist.] 2013, orig. proceeding), the appeals court stated that the "trial court's December 18, 2012, amended order did not provide guidelines as to how [Defendant's] expert would protect relators' privacy and confidentiality or handle privileged documents Accordingly, we hold that the trial court abused its discretion in compelling relators to turn over their computer and network server hard drives" Both *In re Weekley Homes* and *Pinnacle Engineering* provide guidance on what is required to protect the privacy and privilege of information stored on hard drives before an order should be granted to produce such materials.⁸¹

In the criminal context, Texas courts have permitted the disclosure to police of private, potentially criminal data found by someone who has been granted access to the drive by the owner. For example, in the case of *Signorelli v. State*, a computer repairman was given access to a hard drive by the owner.⁸² In the ordinary course of the

^{78.} *E.E.O.C. v. Simply Storage Management, LLC*, 270 F.R.D. 430, 440 (S.D. Ind. 2010) ("SNS [social networking site] content is not shielded from discovery simply because it is 'locked' or 'private.' Although privacy concerns may be germane to the question of whether requested discovery is burdensome or oppressive and whether it has been sought for a proper purpose in the litigation, a person's expectations and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery. . . . As in other cases when privacy or confidentiality concerns have been raised, those interests can be addressed by an appropriate protective order, like the one already entered in this case.").

^{79.} In re Weekley Homes, 295 S.W.3d at 311.

^{80.} In re Weekley Homes, 295 S.W.3d at 318. See also In re Shipman, 540 S.W.3d 562 (Tex. 2018) (the trial court order contained a "detailed forensic examination protocol to protect [the individual's] privacy and legal privileges." The forensic examiner would "blindly" generate a listing of all file names on the media and provide that list to the individual's counsel, who could object prior to the files being turned over to opposing counsel.)

repairs, he opened files on the computer and discovered evidence of child pornography. He reported this to the local police department, which dispatched an officer to seize the computer. The court held that evidence obtained in this way was admissible; it was reasonable for the police to believe that the repairman had permission to access the system, and the State was also able to show that the owner had taken no steps to encrypt or otherwise protect the data from disclosure.

§ 24.6:6 Other Sources of Private Information

A variety of other sources of private information have been addressed in Texas and federal courts. By way of example, the following list provides a brief overview of some of these decisions.

- The Driver's Privacy Protection Act protects state motor vehicle records from use by attorneys for solicitation of clients (*Maracich v. Spears*, 570 U.S. 48 (June 17, 2013))
- Bank account information and telephone numbers generally not discoverable (*Indigital Solutions, LLC v. Mohammed*, Civ. No. H-12-2428, 2012 WL 5825824 (S.D. Tex. Nov. 15, 2012))
- Cell phone records are discoverable (*Wright v. Weaver*, No. 4:07-CV-369, 2009 WL 5170218 (E.D. Tex. Dec. 18, 2009))⁸³
- Securities customers' purchases are potentially discoverable (*Shanklin v. Columbia Management Advisors, L.L.C.*, Civ. No. H-07-2690, 2009 WL 1351798 (S.D. Tex. May 13, 2009))

82. No. 09-06-450 CR, 2007 WL 4723210 (Tex. App.—Beaumont Jan. 16, 2008, pet. ref'd) (mem. op., not designated for publication).

^{81.} Citing both *Weekley* and *Pinnacle*, the Dallas court of appeals in *In re VERP Inv., LLC*, 457 S.W.3d 255, 263 (Tex. App.—Dallas 2015) (citations omitted) summarized the standard as follows: "Even in cases in which the responding party has been shown to have defaulted on its discovery obligations, direct access to the electronic storage devices is not automatic. Once a court has determined that the nature of the case requires direct access to an electronic storage device, if it is not possible for the trial court to describe search protocols with sufficient precision to capture only relevant, nonprivileged information, the trial court may order the forensic examination to be performed by an independent third-party forensic analyst. Only a qualified expert should be afforded such access and only when there is some indication that retrieval of the data sought is feasible."

^{83.} In contrast, the Beaumont court of appeals denied a request for a forensic examination of a cell phone in a motor vehicle personal injury case when the relator sought all stored and deleted photos, videos, e-mails, texts, and other electronic communications (*In re Indeco Sales, Inc.*, No. 09-14-00405-CV, 2014 WL 5490943 (Tex. App.—Beaumont, Oct 30, 2014). The court found the request was "overbroad, not properly limited in time and scope, and constituted an unwarranted intrusion" (citing *Weekley* and *Christus*).

- Stockholder status is discoverable (*In re Union Energy, Inc.*, No. 12-08-00305-CV, 2008 WL 4757008 (Tex. App.—Tyler Oct. 31, 2008, orig. proceeding) (mem. op.)
- Nonparty policyholder information is discoverable (*In re Kemper Lloyds Ins. Co.*, No. 12-05-00309-CV, 2006 WL 475436 (Tex. App.–Tyler, Feb. 28, 2006, orig. proceeding) (mem. op.))
- Personnel files may be discoverable if a party fails to make a proper factual showing that the information sought is protected by the claimed privacy interest; general assertions of privilege are not sufficient, and the trial court did not abuse its discretion by allowing disclosure without conducting an in camera review. (*In re Crestcare Nursing & Rehabilitation Center*, 222 S.W.3d 68 (Tex. App.—Tyler 2006, orig. proceeding))
- Personnel file was shown to contain Social Security number, medical information, and home address, and must be redacted before it is disclosed (*Frierson v. City of Terrell*, No. 3:02-CV-240-H, 2003 WL 21955863 (N.D. Tex. Aug. 15, 2003))

§ 24.7 Restrictions (Redaction, Protective Orders, Confidentiality Agreements)

Production of personal or private information may be allowed if the documents are redacted to excise the private information. Redaction is more likely to be allowed if the private information is not relevant, as redaction of nonresponsive information contained in responsive documents is becoming more acceptable in the courts.⁸⁴ Particularly for irrelevant personal or sensitive information, the redaction of nonresponsive personal information is an important safeguard from possible disclosure to third parties. In *In re Takata Airbag Products Liability Litigation*, the defendants argued they should have been allowed to redact irrelevant sensitive information could be disclosed to competitors.⁸⁵ The court agreed and noted that under rule 26(b)(1) of the Federal Rules of Civil Procedure, "a party is not entitled to receive every piece of relevant information. It is only logical, then, that a party is similarly not entitled to receive every piece of irrelevant information in responsive documents if the producing party has a persuasive reason for why such information should be withheld."⁸⁶

^{84.} See In re Takata Airbag Prod. Liab. Litig., No. 14-24009-CV, 2016 WL 1460143, at *1 (S.D. Fla. Mar. 1, 2016).

^{85.} In re Takata, 2016 WL 1460143, at *1

Privacy Issues

One such persuasive reason could easily be privacy, particularly for nonparties who are not interested in the litigation like consumers, customers, and employees.

Whether the use of redaction is sufficient will depend on the case, and practitioners should be aware that redaction is not always appropriate or sufficient to overcome privacy and privilege concerns. For example, in a dispute between an insured and his two insurance companies, the plaintiff requested the production of medical peer review reports of nonparties.⁸⁷ Under a strict reading of Texas Rule of Evidence 509(c) and the Texas Medical Practice Act (Tex. Occ. Code § 159.002(a)–(c)), the San Antonio court of appeals held that peer reports concerning third parties created by doctors at the request of the defendant were not discoverable. ⁸⁸ Moreover, the court held that redacting the identities of the patients in these reports did not make them discoverable. Both rule 509 and section 159.002(a)–(c) forbid disclosure of records detailing "the identity, diagnosis, evaluation, or treatment of a patient."⁸⁹ Upholding Texas precedent, the court held that "[t]he redaction of the nonparties' identifying information does not address the privilege as it applies to the diagnosis, evaluation, or treatment of the patient."⁹⁰

A court may order parties to enter into a confidentiality agreement in addition to the use of redaction.⁹¹ Addressing the privacy interests of nonparties regarding drug and medication records, the United States District Court for the Southern District of Texas, arriving at a conclusion contrary to the San Antonio Court of Appeals in *In re Netherlands Insurance*, found redaction of personally identifiable information to be an adequate protection, allowing discovery of records where the defendant was alleged to have incorrectly filled prescriptions.⁹² Coupled with a confidentiality agree-

86. In re Takata, 2016 WL 1460143, at *2.

87. In re Netherlands Ins. Co. & American First Ins. Co., No. 04-08-00815-CV, 2009 WL 962539 (Tex. App.—San Antonio Apr. 8, 2009, orig. proceeding).

- 88. In re Netherlands Insurance Co., 2009 WL 962539, at *3.
- 89. In re Netherlands Insurance Co., 2009 WL 962539, at *3.
- 90. In re Netherlands Insurance Co., 2009 WL 962539, at *4.

91. See Riley v. Walgreen Co., 233 F.R.D. 496, 501 (S.D. Tex. 2005) (In response to plaintiff's request for prescription patient information, the court stated "[g]iven the extremely sensitive information at issue, the court agrees that both redaction of names and a confidentiality agreement are appropriate. Riley's objection to redaction, i.e., that it would hinder further investigation into matters relevant to exemplary damages, is blunted by the fact that Walgreen will be required to provide names of complaining customers (without reference to their particular prescriptions) in response to Interrogatory No. 1. Production of prescription records segregated from customer names, under the auspices of a confidentiality agreement, achieves the appropriate balance between plaintiff's legitimate discovery needs and the protection of third party medical records.").

92. Riley, 233 F.R.D. at 501.

ment, the court held that "[p]roduction of prescription records segregated from customer names achieves the appropriate balance between Plaintiff's legitimate discovery needs and the protection of third party medical records."⁹³ The court further held that the privacy interests of defendant employees in their personnel records would be adequately protected by confidentiality agreements alone.⁹⁴

Use of redaction may be coupled with a protective order to ensure protection of private information. In a case in which the plaintiff demanded financial information that could also result in the production of private patient information from a medical device maker, the court stated that—

to the extent that any documents requested happen to include a patient's identity, diagnosis, treatment, or evaluation unrelated to the . . . clinical trial, that information should be redacted and any remaining portions subject to a protective order . . . The combination of redaction and protective order is consistent with the purposes of the [physician-patient] privilege to allow for open communications without fear of disclosure, so that the physician can effectively treat the patient. *See In re Rezulin Prods. Liab. Litig.*, 178 F. Supp. 2d 412, 415 (S.D.N.Y. 2001) (interpreting Texas law and determining "[o]nce information cannot be connected with patient, the risk of embarrassment that might lead a patient to withhold information from a physician and thus interfere with proper treatment, as well as the risk of any invasion of personal privacy, is eliminated").⁹⁵

§ 24.8 International Data Protection Laws

If discovery is propounded in a case that implicates information that resides in a non-U.S. jurisdiction, attorneys must take precautions that requirements for the processing and disclosure of private information of foreign nationals are met. In the leading Supreme Court case on this issue, the court discussed how a balancing exercise should be carried out with the aim that the trial court should rule on a party's request for production of information located abroad only after balancing certain factors.

^{93.} Riley, 233 F.R.D. at 501.

^{94.} Riley, 233 F.R.D. at 501.

^{95.} *Timberlake v. Synthes Spine Co., L.P.,* No. V-08-4, 2008 WL 2770588 (S.D. Tex. June 4, 2008) (order granting in part and denying in part protective order). *See also Vann v. Mattress Firm,* No. H-12-3566, 2014 WL 1365943 (S.D. Tex. Apr. 7, 2014) ("The court will not require Mattress Firm to disclose such information from personnel files until a protective order is in place.").

Privacy Issues

Société Nationale Industrielle Aerospatiale v. United States District Court for Southern District of Iowa, 482 U.S. 522 (1987).

Although U.S. interest in relevant discovery generally trumps foreign privacy laws⁹⁶ that would prevent disclosure, international discovery disputes require U.S. courts to "exercise special vigilance,"⁹⁷ and some courts have denied such discovery or have exercised their discretion to require the requesting party to first exhaust the Hague Convention's discovery procedures.⁹⁸

With the implementation of the General Data Protection Regulation ("GDPR") in the EU on May 25, 2018, the tension between U.S. discovery and foreign privacy laws has only exacerbated. The GDPR is a mandatory regulation that limits how personal information of EU citizens is maintained, processed, used, or transferred. Violations of the GDPR's transfer provisions can bring forth administrative fines of up to 20 million euros or four percent of the violating company's annual worldwide revenue, whichever is higher.⁹⁹ While the GDPR does allow for the processing of data to be compliant with legal obligations, that allowance is only for EU member states.¹⁰⁰ In addition, some courts have already been reluctant to find that the GDPR provides adequate reason to not produce documents.¹⁰¹ Essentially, litigants may find themselves having to choose between the consequences of noncompliance with a U.S. court order, or being hit with fines from European regulators for noncompliance with the GDPR.

In Texas, the case of *Volkswagen AG v. Valdez* provides a helpful analysis of the factors Texas courts will assess to determine if a party must produce protected, private information in the possession of its foreign operations.¹⁰² A detailed discussion of the

99. GDPR, Art. 83(5).

100. GDPR, Recital 45.

^{96.} See Royal Park Investments SA/NV v HSBC Bank USA, N.A., No. 14 Civ. 8175 (LGS), 2018 WL 745994, at *1 (S.D.N.Y. Feb. 6, 2018) (ruling that comity weighed in favor or producing documents as opposed to the Belgium Privacy Act).

^{97.} Aerospatiale, 482 U.S. at 546. Courts need to consider the additional cost and burden of conducting cross-border discovery. U.S. rules require that documents sought be incrementally more valuable in order for the discovery to be proportionate and not outside the scope of discovery. *See In re Bard IVC Filters Prod. Liab. Litig.*, 317 F.R.D. 562, 566 (D. Ariz. 2016).

^{98.} See, e.g., Salt River Project Agric. Improvement & Power Dist. v. Trench France SAS, 303 F. Supp. 3d 1004, 1010 (D. Ariz. 2018) (ruling that there was hardship to French defendant due to French blocking statute and allowing discovery to move forward under the Hague Convention).

^{101.} See Finjan, Inc. v. Zscaler, Inc., No. 17CV06946JSTKAW, 2019 WL 618554, at *3 (N.D. Cal. Feb. 14, 2019) (ruling that the GDPR did not preclude the Court from ordering Defendant to produce the requested e-mails in an unredacted form).

issues related to the protection and disclosure of information residing in a non-U.S. jurisdiction is beyond the scope of this chapter,¹⁰³ and a number of helpful resources related to these complex issues are now available.¹⁰⁴

^{102. 897} S.W.2d 458 (Tex. App.—Corpus Christi–Edinburg 1995, orig. proceeding), *mand. granted*, *Volkswagen AG v. Valdez*, 909 S.W.2d 900 (Tex. 1995) (per curiam) (court held that the trial court abused its discretion in failing to balance the competing interests of the parties and by disregarding German privacy laws, and concluded the information sought should not be produced).

^{103.} See chapter 23 of this book.

^{104.} For examples, see The Sedona Conference, International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation, Vol. 19, No. 2 (2018), https://thesedonaconference.org/sites/default/files/publications/International%20Investigations%20Principles%20%282018%29. pdf.

Chapter 25

ESI Discovery in Texas Criminal Practice

Eric J. R. Nichols¹

§ 25.1 Introduction—The Paradigm Shift

Over the past twenty years, computers and the Internet have revolutionized business, including the business of the investigation, prosecution, defense, and trial of criminal cases. The transition from a largely paper-based world to a world in which most information is created and stored electronically has drastically changed the practice of litigation generally. There is no doubt that this shift has been felt to a larger degree in civil litigation than in criminal litigation. But the effects of technology have been felt on both dockets. For example, in 1993 only five percent of discoverable documents were derived from an electronic source.² By 2008, a mere fifteen years later, more than ninety-three percent of all business documents were created electronically.³ That percentage has only increased in the last decade. As another commentator has summarized: "Digital evidence in criminal cases is exploding."⁴

Civil litigators were first to recognize the importance of developing and employing effective strategies to manage electronically stored information ("ESI"), and as discussed elsewhere in this book, the Federal Rules of Civil Procedure were amended as early as 2006 to address issues unique to electronic discovery. Criminal lawyers (both prosecutors and defense counsel) have only in more recent years recognized the importance of managing ESI effectively, and both the discovery provisions of Federal Rules of Criminal Procedure and protocols used by criminal law practitioners have yet to fully catch up (and may never fully catch up) to their civil counterparts on the e-

^{1.} The author gratefully acknowledges the tremendous substantive contributions to this chapter by Marla Cadeddu, who coauthored the chapter for a prior edition of this publication; Don Flanary, who practices criminal defense in San Antonio; and the many other criminal law practitioners (both prosecutors and defense counsel) who provided input for the topic of this chapter.

^{2.} Vlad J. Kroll, Default Production of Electronically Stored Information Under the Fed. Rules of Civil Procedure: The Requirements of Rule 34(b)(ii), 59 Hastings L.J. 221 (2005).

^{3.} Albert J. Marcella Jr., *Electronically Stored Information and Cyberforensics*, 5 Info. Sys. Control J. 2 (2008), available at: https://audit4security.com/wp-content/uploads/2020/02/Electronically -Stored-Information-Cyber-Forensics.pdf.

^{4.} Jenia I. Turner, *Managing Digital Discovery in Criminal Cases*, 109 J. Crim. L. & Criminology 237, 239 (2019).

discovery front. Indeed, as summarized by the Federal Judicial Center in a publication to federal judges:

The rules governing civil and criminal discovery are fundamentally dissimilar due to the different public policies underlying criminal and civil litigation, constitutional requirements, and special ethical obligations of prosecutors and defense counsel. Consequently, courts have generally refrained from applying civil e-discovery rules to criminal discovery.⁵

There continues to be progress on the criminal justice side of e-discovery, however. This is reflected in the addition of a new section to the Federal Rules of Criminal Procedure, set to take effect on December 1, 2019. This new rule, as discussed below, sets a framework for discussions between federal prosecutors and criminal defense counsel about the format and timing of discovery, including e-discovery in the appropriate case. The new rule also sets a framework and the timing of court intervention as needed as prosecutors and criminal defense counsel attempt to resolve the issues.

§ 25.1:1 Joint Electronic Technology Working Group ESI Protocol

This recent change to the Federal Rules of Criminal Procedure builds on, and is a natural progression of, the effort to address the unique issues regarding ESI in federal criminal cases. These issues began with the Joint Electronic Technology Working Group that was formed by the director of the Administrative Office of the U.S. Courts and the U.S. Attorney General. The Working Group included representatives of the Administrative Office, the U.S. Department of Justice, federal public and community defender offices, and private attorneys who accept Criminal Justice Act (CJA) appointments. Following two years of study and analysis, in February of 2012 the Working Group issued "Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases," also known as the "ESI Protocol."⁶ The ESI Protocol was sent in 2012 by a deputy attorney general to all U.S. attorney offices, and by the Administrative Office to all federal defenders and CJA panel attorneys.⁷

^{5.} Federal Judicial Center, Criminal E-Discovery: A Pocket Guide for Judges (2019), www.fjc.gov/sites/default/files/materials/06/Criminal%20e-Discovery_First%20Edition_Third% 20Printing_2019.pdf, p. 2.

^{6.} Joint Working Group, Electronic Technology in the Criminal Justice System, Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases (Feb. 2012), www.fd.org/sites/default/files/Litigation%20Support/final-esi-protocol.pdf (hereinafter "ESI Protocol").

The ESI Protocol provides guidance to both prosecutors and defense counsel for managing ESI disclosures in criminal cases in an efficient and cost-effective manner. Although the ESI Protocol borrows from the civil practice experience, it seeks to address issues that are unique to criminal cases. Importantly, however, in contrast to the civil arena in which ESI collection, disclosure, and management are now governed by binding federal rules, the ESI Protocol consists merely of a collection of nonbinding recommendations and strategies. Nonetheless, as compared to the ad hoc, case-by-case approach that preceded it, the ESI Protocol gives the parties and courts some direction regarding how best to manage ESI in the criminal context and is a seminal development in federal criminal trial practice.

§ 25.1:2 Other Agency Protocols and Instructions

In addition, reported case decisions on e-discovery practices in criminal cases have continued to be generated, albeit at a much lower rate than in the civil justice system, for obvious reasons. Large-scale e-discovery issues arise in only a limited number of federal criminal prosecutions, such as cases involving "white collar" fraud charges or cases involving cyber threats, terrorism, or extortion. Of course, in an age of smart-phones that contain vast amounts of ESI and electronic storage capacity, smaller-scale e-discovery issues can occur in almost any federal criminal prosecution. A relatively small number of disputes related to federal criminal e-discovery have made their way into published decisions, much less in decisions published at a level beyond a federal district court. As discussed in this chapter, those limited published case decisions have also added to the ESI protocol in terms of the guidance available to criminal law practitioners and to courts faced with e-discovery issues in actual prosecutions.

On the other hand, ESI issues are often encountered by investigators, prosecutors, and criminal defense attorneys in the context of "white collar" fraud investigations including government program fraud and securities fraud matters—and criminal investigations related to cyber fraud, theft, and extortion. As discussed in this chapter, federal law enforcement agencies have oftentimes established widely employed written guidelines and instructions for the production of ESI in response to document requests made in agency administrative and grand jury subpoenas. These protocols and instructions, which are often made available on an agency's website and often attached to such subpoenas, set out suggested formats and parameters for production of ESI. The agencies' own guidelines and instructions may also help to inform the

^{7.} See announcement from the Administrative Office of U.S. Courts, www.uscourts.gov/news/ 2012/04/23/ao-justice-department-jointly-recommend-esi-discovery-practices.

resolution of e-discovery disputes, not only in the context of subpoena responses but also in post-indictment criminal discovery.

The implementation of enhanced e-discovery platforms for federal criminal cases has also from time to time been the subject of U.S. Department of Justice appropriation requests.⁸ Such requests reflect an effort to promote and fund a consistent approach to the collection, analysis, and potential e-discovery of ESI across the Department of Justice and United States Attorneys' offices, and give at least some insight into how the Department of Justice views and internally approaches issues of ESI collection and storage. However, practitioners are likely to find ESI collection, storage, and production techniques that differ according to the investigating agency, the particular U.S. Attorney's office, and perhaps even the individual prosecutor within that U.S. Attorney's office involved in the case.

§ 25.1:3 Texas State Courts

Texas state courts have yet to adopt any guidelines specific to discovery of electronic information in criminal cases, such as those set out in the recent change to the Federal Rules of Criminal Procedure or the ESI Protocol. The Texas Code of Criminal Procedure has only in the past several years been amended in a manner that begins to recognize that ESI discovery issues may exist in a case. Since that legislative change, several prosecutor offices across the state have implemented e-discovery protocols and platforms, but practices within individual Texas prosecution jurisdictions vary to significant degrees. As a result, state criminal practitioners encounter treatments of ESI discovery that vary as much or even more from prosecutor to prosecutor, court to court, and case to case in state criminal proceedings than in federal courts.

This chapter first addresses the ever-evolving federal practices on ESI discovery, and then provides a general framework for how Texas prosecutors dealing with ESI discovery and Texas state courts hearing criminal cases have dealt with ESI discovery matters in the past, and how courts, prosecutors, and defense attorneys may choose to deal with these evolving issues in the future.

^{8.} FY 2017 Performance Budget Congressional Submission, United States Attorneys, available at: www.justice.gov/about/fy-2017-congressional-budget-submission.

§ 25.2 Federal Rule of Criminal Procedure 16.1—2019 Amendment

An amendment to the Federal Rules of Criminal Procedure, enacted and made effective as of December 1, 2019, puts some structure on the types of discussions that routinely occur in federal criminal cases. New rule 16.1⁹ requires that a discussion about "the timetable and procedures for pretrial disclosure" occur within fourteen days of federal court arraignment.¹⁰ Next, the new rule explicitly authorizes a party—following such a conference—to seek court intervention by asking the court to "determine or modify the time, place, manner, or other aspects of disclosure" of discovery.¹¹

This rule obviously does not mandate any particular form of e-discovery, much less the substance of discovery to be provided. With respect to e-discovery, the rule's comments make this plain:

Because technology changes rapidly, the rule does not attempt to state specific requirements for the manner or timing of disclosure in cases involving ESI. However, counsel should be familiar with best practices. For example, the Department of Justice, the Administrative Office of the U.S. Courts, and the Joint Working Group on Electronic Technology in the Criminal Justice System (JETWG) have published "Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases" (2012).

Fed. R. Crim. P. 16. The advisory committee further indicated in its report to the United States Supreme Court—which in turn adopted the rule change by an April 2019 order—that the consensus of the committee (made up of judges and practitioners) was that "the rule should be simple and place the principal responsibility for implementation on the lawyers."¹² The advisory committee's report also indicates that a broader rule to govern discovery in complex cases, including ESI, was considered but then rejected in favor of the more "simple" rule as enacted.¹³ In particular, "Itlhe

12. United States Supreme Court Order (Apr. 25, 2019) and excerpt from the September 2018 Report of the Committee on Rules of Practice and Procedure (Sept. 2018), www.fjc.gov/sites/default/ files/materials/56/2019-04-25-congressional_rules_package_final_0.pdf.

^{9.} The new rule states: "(a) Discovery Conference. No later than 14 days after the arraignment, the attorney for the government and the defendant's attorney must confer and try to agree on a timetable and procedures for pretrial disclosure under Rule 16. (b) Request for Court Action. After the discovery conference, one or both parties may ask the court to determine or modify the time, place, manner, or other aspects of disclosure to facilitate preparation for trial."

^{10.} Fed. R. Crim. P. 16.1(a) (eff. Dec. 1, 2019).

^{11.} Fed. R. Crim. P. 16.1(b).

prosecutors and Department of Justice attorneys also felt strongly that any rule must be flexible given the variation among cases."¹⁴

The inclusion of "determine or modify" within the section of the new rule 16.1 that addresses potential court intervention is intended to cover both situations in which (1) no court order (standing order or otherwise) or local rule addresses a discovery schedule in the case, and (2) there is a court order or local rule and one side or the other feels modification is necessary in that case.¹⁵ In a manner consistent with the advisory committee's conclusion that "one size does not fit all" for criminal discovery—including e-discovery—the rule thus provides flexibility to counsel on either side of the case to raise particular issues specific to the case to the court for resolution.

The manners in which this flexibility can be exercised are now readily apparent. For example, a prosecutor in a complex case can seek relief from a deadline applied by an existing court-ordered or standing order deadline to complete pretrial disclosures to the defense. Defense counsel who are not able to get prosecutors to agree to a particular format of production that in their view would be readily reviewable and usable, or to get prosecutors to agree to what they view as acceptable timing of disclosure of e-discovery, now have an explicit platform in the rules to seek intervention and ruling by a district court. The government obviously has an interest in attempting to reach resolution of e-discovery issues before they are brought to a court's attention, and defense counsel may be motivated to reach resolution as well.¹⁶ Regardless, courts are undoubtedly gaining an increased appreciation for the complexities of such e-discovery issues as:

- the format of various types of ESI maintained by prosecutors and the agencies with which they work;
- the transfer of ESI by the government to defense counsel;
- the loading of ESI by defense counsel into particular review platforms;

^{13.} United States Supreme Court Order (Apr. 25, 2019) and excerpt from the September 2018 Report of the Committee on Rules of Practice and Procedure (Sept. 2018).

^{14.} United States Supreme Court Order (Apr. 25, 2019) and excerpt from the September 2018 Report of the Committee on Rules of Practice and Procedure (Sept. 2018).

^{15.} United States Supreme Court Order (Apr. 25, 2019) and excerpt from the September 2018 Report of the Committee on Rules of Practice and Procedure (Sept. 2018).

^{16.} Jenia I. Turner, *Managing Digital Discovery in Criminal Cases*, 109 J. Crim. L. & Criminology 237, 241 (2019).

- the need for prosecutors to make fulsome disclosures to discharge their responsibilities; and
- the need for criminal defense counsel to make rational and reasonable efforts to encounter and review produced ESI for purposes of providing a defense to their clients.

The new rule recognizes that district courts have already engaged in discussions about ESI in federal criminal cases and anticipates that if called upon to do so, a district court will tailor a discovery plan and schedule to the particular matter. How this new rule plays out—in terms of the frequency of e-discovery motions and hearings—has yet to be seen. However, the availability and engagement of the district court—through the district judge or an assigned magistrate judge¹⁷—will be crucial as the parties work through e-discovery issues in complex cases, and may well result in additional discovery conferences and status conferences so that the district court can provide guidance and "call balls and strikes" as the parties work through those issues.¹⁸

§ 25.3 ESI Protocol—Description and Application

As the parties do work through e-discovery issues, including through the framework set out in the new addition to the Federal Rules of Criminal Procedure, the ESI Protocol will often come into play. The comments to newly enacted rule 16.1 make explicit reference to the ESI Protocol. The ESI Protocol provides a framework for (1) communications between the parties regarding ESI, (2) managing ESI discovery production, and (3) resolving disputes. Certain fundamental principles animate the ESI Protocol. Among these principles, and in a manner carried forward under the new rule 16.1, the ESI Protocol establishes the nondelegable duty of lawyers to understand ESI. Indeed, the ESI Protocol states, "[1]awyers have a responsibility to have an adequate understanding of electronic discovery."¹⁹ At the same time, the Working Group recognized

^{17. 28} U.S.C. § 636(b)(1)(A) (statutory authority for magistrate judges to "hear and determine any pretrial matter" such as discovery matters, subject to specified exceptions and "clearly erroneous" review by the district court).

^{18.} Although the issue has not been thoroughly litigated in the courts, there is also an indication that some district courts may be inclined to use their inherent authority (and possibly even their authority under the Federal Rules of Civil Procedure) to appoint special masters on discovery issues. *See, e.g., Schwimmer v. United States*, 232 F.2d 855, 864–65 (8th Cir.), *cert. denied*, 352 U.S. 833 (1956); *United States v. Black*, No. 16-20032-JAR, 2016 WL 6967120 (D. Kan. Nov. 29, 2016). In a particularly complicated or contentious case, the appointment of a special master may be an option. Of course, the appointment of special masters to handle such complex discovery issues as collection and production of ESI is not uncommon in civil cases.

^{19.} ESI Protocol, Recommendations, p. 2.

the reality that the disclosure and management of ESI is a highly technical endeavor. The ESI Protocol accordingly counsels that "in the process of planning, producing, and resolving disputes about ESI discovery, the parties should include individuals with sufficient technical knowledge and experience regarding ESI."²⁰ Recognizing that ESI technical assistance is costly, the ESI Protocol expressly provides that no party producing ESI should be required to incur additional conversion or processing costs beyond those incurred or planned for its own case.²¹ Additionally, as is now codified in the Federal Rules of Criminal Procedure, parties should meet and confer in good faith to discuss appropriate ESI production formats that maintain data integrity, minimize expense, and conform to industry standards and to resolve ESI disputes.²²

The ESI Protocol seeks to balance several goals. First, of course, is the need of the parties to comply with their respective discovery obligations.²³ In addition however, the ESI Protocol seeks to address the proliferation of electronic data and the complexities that the sheer volume of data may impose on the parties to a criminal case, including the impossibility of document-by-document review in large-volume ESI cases.²⁴ In that regard, the ESI Protocol notes:

[T]he volume of ESI in many cases may make it impossible for counsel to personally review every potentially discoverable item, and, as a consequence, the parties increasingly will employ software tools for discovery review, so ESI discovery should be done in a manner to facilitate electronic search, retrieval, sorting, and management of discovery information.²⁵

Relatedly, another important goal of the ESI Protocol is to ensure production of ESI in industry-standard format while avoiding unnecessary duplication of effort and expense.²⁶ All the while, the ESI Protocol recognizes that the protection of privileged data, work product, or classified or otherwise confidential information is paramount.²⁷

The ESI Protocol does not apply in every case. Nor does it alter the parties' discovery obligations or create new rights or privileges.²⁸ A critically important consideration is

- 22. ESI Protocol, Introduction, pp. 1-2.
- 23. ESI Protocol, Recommendations, p. 1.
- 24. ESI Protocol, Recommendations, at 1.
- 25. ESI Protocol, Recommendations, at 1.
- 26. ESI Protocol, Recommendations, at 1.
- 27. ESI Protocol, Recommendations, at 1.

^{20.} ESI Protocol, Introduction, p. 1.

^{21.} ESI Protocol, Introduction, p. 2.

ESI Discovery in Texas Criminal Practice

that unlike in the civil context in which a violation of the Federal Rules of Civil Procedure is potentially sanctionable, the ESI Protocol expressly provides that it cannot be used as a basis for misconduct claims or other claims for relief by either party.²⁹

The ESI Protocol has a tripartite structure. First, in the initial Recommendations section, it outlines a general framework and suggested work process for both the defense and prosecution to follow in handling ESI in a federal criminal case. Second, the ESI Protocol provides Strategies and Commentary, including practical technical guidance and useful definitions of terms likely to be encountered when dealing with ESI. Finally, and perhaps most importantly, the ESI Protocol includes a checklist for attorneys to follow when dealing with criminal ESI.

As an example, the treatment of the meet and confer process in the ESI Protocol illustrates the interconnectedness of the different sections. The Recommendations section of the ESI Protocol provides that the parties should discuss and jointly decide the format for production of ESI, ensuring that formats conform to industry standards.³⁰ The Strategies and Commentary section of the ESI Protocol includes an exhaustive list of potential categories of ESI discovery including investigative materials, witness statements, documentation of tangible object seizures, digital devices and records of third parties, photographs and audio recordings, Title III wiretap information, court records, tests and examinations, expert-related information, immunity and plea agreements, discovery materials with special handling or production considerations, and miscellaneous other items such as data from parallel proceedings or investigations and materials that will not be produced digitally.³¹ Finally, the ESI Discovery Production Checklist walks counsel stepwise through issues to be addressed during the meet and confer process.³²

Regarding the production of ESI, under the Recommendations section of the protocol, ESI received from third parties and the parties' own business records should be produced either in the format in which they were received or in a "reasonably usable format," a term borrowed from Federal Rule of Civil Procedure 34(a)(1)(A).³³ The

- 30. ESI Protocol, Recommendations, p. 3.
- 31. ESI Protocol, Strategies, pp. 1–2.
- 32. ESI Protocol, ESI Discovery Production Checklist.

^{28.} ESI Protocol, Recommendations, at 1. Indeed, the Protocol notes, "[t]he Recommendations and Strategies are intended to apply only to disclosure of ESI under Federal Rules of Criminal Procedure 16 and 26.2, *Brady*, *Giglio*, and the Jencks Act." Moreover, the Protocol does not apply to civil or criminal investigations. ESI Protocol, Recommendations, p. 1 n.1.

^{29.} ESI Protocol, Recommendations, p. 2.

production of electronic documents should arguably be made in industry-accepted formats; for example, producing documents stored as PDF in a way that can be discerned as document units and searched.³⁴ Although the ESI Protocol recommends that in the production of ESI to the other party, no party should be compelled to incur additional processing or formatting costs beyond those already incurred or anticipated for its own case preparation, once a party processes ESI it should produce the results of that processing along with the underlying ESI as a cost-saving measure.³⁵ Furthermore, to avoid e-discovery formatting and organizational issues, the government may decide to affirmatively organize e-discovery in a manner that corresponds to the charges made against multiple defendants in a complex case. For example, in *United States v. Cadden*:

Each production was provided on a hard drive or discs. The electronic documents were generally organized into folders, as well as searchable loadready electronic databases. The initial discovery production included a folder labeled "Indictment Counts," which contained records and documents relevant to the 131 counts in the indictment, organized by count. The first two discovery productions were accompanied by spreadsheets identifying "hot" and "relevant" records and documents within the electronic databases. In addition, each production was accompanied by detailed letters describing the information provided in the production, the location where the information was stored on the hard drive or discs, and the corresponding Bates range of the information.³⁶

However, the ESI Protocol itself would not appear to require the government to undertake this level of effort.

The ESI Protocol also exempts from its disclosure recommendations discovery generated by the government or the defense during the course of investigations—for example, investigative reports and reports of interview—noting that the parties may handle

^{33.} ESI Protocol, Recommendations, at 3.

^{34.} See, e.g., United States v. Soliman, No. 06CR236A 2008 WL 4490623, at *4 (W.D.N.Y. Sept. 30, 2008) (ordering the government to reproduce electronic records in a format that had an identification system for individual documents and allowed documents to be "readily retrievable"); see also United States v. Fattah, 223 F. Supp.3d 336 (E.D. Pa. 2015) and United States v. O'Keefe, 537 F. Supp.2d 14 (D.D.C. 2008) for the proposition that the government should produce electronic documents in a format that tracks the original constitution of the records and is searchable).

^{35.} ESI Protocol, Recommendations, pp. 3-4.

^{36.} United States v. Cadden, No. 14-10363-RGS, 2015 WL 13683814, at *1 (D. Mass. July 13, 2015), report and recommendation adopted in part and rejected on other grounds, 2015 WL 5737144 (D. Mass. Sept. 30, 2015).

such materials differently than other ESI discovery.³⁷ However, production of postprocessed ESI is subject to the limitation that work product need not be produced.³⁸ The ESI Protocol provides guidance as to production methodologies that the parties may consider in determining how a party will produce paper documents that are to be converted to digital format.³⁹

The ESI Protocol also addresses the mechanism of transmission of ESI discovery from one party to the other. Again, transmission issues should be addressed during the meet and confer. Importantly, however, the ESI Protocol provides that "ESI discovery should be transmitted on electronic media of sufficient size to hold the entire production, for example, a CD, DVD, or thumb drive."⁴⁰ This provision would seem to preclude transmittal of ESI production on dozens of CDs or DVDs, encouraging instead transmittal on a large-capacity hard drive, the cost of which may be borne by the receiving party.⁴¹ The ESI Protocol mandates that all media should be clearly labeled and should be accompanied by a cover letter detailing the contents of the production as well as any additional information necessary to access the data.⁴² The ESI Protocol encourages a producing party to create a table of contents "describing the general categories of information available as ESI discovery."⁴³

Interestingly, the ESI Protocol also provides for the appointment of a coordinating discovery attorney in multi-defendant federal criminal cases.⁴⁴ A coordinating discovery attorney is authorized to accept discovery on behalf of all defendants, may assist in the preparation of budgets and funding requests for experts to manage ESI and in negotiating the format of ESI production and transmission, and may otherwise assist the defense in managing ESI discovery.⁴⁵

- 37. ESI Protocol, Recommendations, at 3-4.
- 38. ESI Protocol, Recommendations, at 3-4.
- 39. ESI Protocol, Strategies, pp. 6-7.
- 40. ESI Protocol, Strategies, p. 10.
- 41. ESI Protocol, Strategies, at 10.
- 42. ESI Protocol, Strategies, at 10.
- 43. ESI Protocol, Strategies, at 2.
- 44. ESI Protocol, Recommendations, p. 4; ESI Protocol, Strategies, p. 11.
- 45. ESI Protocol, Strategies, p. 11.

§ 25.4 Implementation of ESI Discovery Platforms and Guidelines by the Department of Justice and Federal Agencies

The implementation of the ESI Protocol's goals and objectives by federal prosecution offices has proven, for obvious reasons, to be complicated. As the Department of Justice indicated in a FY 2017 report on implementation of ESI handling and discovery procedures in its congressional budget submissions:

USAs manage significant amounts of information, including physical evidence, business records, interviews, expert reports, depositions, and witness information. Much of this information is now stored electronically, requiring the USA offices to substantially change their information management systems and the way they collect, process, and produce eDiscovery in their cases. The Department will continue to focus on developing and implementing protocols for handling electronically stored information and to provide specialized training on eDiscovery issues for all attorneys and support staff so they can effectively and efficiently address eDiscovery legal issues and processes.⁴⁶

To be sure, the above language and the corresponding investment applies more directly to resources employed in the civil litigation, both affirmative and defensive, in which a U.S. Attorney's office represents the government or a federal government agency or employee. On the criminal side, criminal prosecutions almost exclusively result from investigations conducted not by a U.S. Attorney's office but instead by one or more federal law enforcement agencies. Each federal law enforcement agency has its own system of databases and forensic software. Federal prosecutors rely on these law enforcement agencies to store and process ESI during the course of investigations and must rely to some degree on the agency to produce ESI from that agency's system in a format that can be used not only by the prosecutor but also—if disclosure is warranted in the case—by the defense.

The parameters of the various systems operated by these various federal law enforcement agencies can be gleaned to some degree from the standard request for delivery of ESI information in federal grand jury and administrative subpoenas.⁴⁷ Under these subpoenas, the Department of Justice or a U.S. Attorney's office (normally in con-

§ 25.4

^{46.} www.justice.gov/jmd/file/822056/download; see also United States Department of Justice, FY 2017 Budget and Performance Summary, U.S. Attorneys, www.justice.gov/about/fy-2017-budget-and -performance-summary.

^{47.} An example of such requests for the format in which ESI is to be delivered to the government is available at: www.justice.gov/archives/dag/page/file/913236/download.

- Images delivered in 300-dpi single-page TIFF files⁴⁸
- Images to be "OCR'd"⁴⁹
- Images to be delivered in folders that correspond to the grouping of pages in a document or "other log_cal grouping"
- Use of image cross reference and "load" files compatible with a particular form of software used by the agency⁵⁰
- Required metadata fields⁵¹

Another example of these requirements is made publicly available by the Securities and Exchange Commission, with respect to its enforcement investigations and inquiries.⁵² Although the formats of the standard requests inevitably contain similarities, there are differences between agencies. As an example, the Commodity Futures Trading Commission requests images be produced in "native file" format rather than a conversion to TIFF images.⁵³

Accordingly, both prosecutors and criminal defense counsel should, as part of the ediscovery process, gain as much knowledge as possible about the format in which the agency or agencies involved in the uncerlying investigation have gathered and stored ESI relevant to the case. For their part, defense practitioners can gain some under-

51. Obviously, as discussed below, metadata (such as that relating to the timing and editing of an electronic image or document) can be of great evidentiary use by both the prosecutor and defense attorney in a particular case.

52. U.S. Securities and Exchange Commission Data Delivery Standards, www.sec.gov/divisions/ enforce/datadeliverystandards.pdf.

53. CFTC Data Delivery Standards (May 26, 2016), www.cftc.gov/sites/default/files/idc/groups/ public/@lrenforcementactions/documents/file/enfdatadeliverystandards052716.pdf. "Native file" format includes, for example, the relatively standard PST format in which many e-mails and instant messages are created.

^{48. &}quot;TIFF" is an industry-recognized acronym for a format known as "Tagged Image File Format."

^{49. &}quot;OCR'd" means placement in a configuration for optical character recognition, which, among other things, allows an image to be word-searched using search terms. In the complex criminal case, this is an obvious and essential tool for filtering through ESI and "data mining."

^{50. &}quot;Cross reference" files allow for the linking of images to a database. "Load" files are text files that contain commands that help import and link data from ESI processing in a database accessed through such programs as Concordance and Summation.

standing from the format of the government's standard request of the ESI material that the government may have in a particular case. It is important to keep in mind that this is not limited to e-mails and other electronic documents, but also photographs and audio and video recordings as well. Several of the agency ESI production guidelines routinely specify formats for electronic photographic image and audio recording data.

Of course, because an agency of the government asks for material in a certain format does not mean that the government actually received material in that format from a person or entity responding to a subpoena,⁵⁴ but practitioners should be sensitive in each case to determining what ESI discovery is potentially available. Practitioners should also keep in mind in the appropriate case that the government collected its data from third parties, such as a corporation or a bank, and that corporation or bank may well have retained a copy of that production to the government. To the extent that a criminal defense practitioner has concerns about the ability or willingness of the government to produce ESI obtained from a particular source (for example, a criminal defendant's current or former employer), a subpoena directed at that source is a potential option. The Federal Rules of Criminal Procedure authorize a party to subpoena a witness (such as a business records custodian) to deliver, among other things, "data."⁵⁵

Getting to the bottom of the data in the possession of the government and the persons and entities from whom federal agencies have collected such data may well be critical to the defense of a case. As one relatively straightforward example, there is no doubt that in the appropriate case it is not only the facial content of electronically stored documents but also the associated metadata that may prove crucial.⁵⁶ Such metadata may be reflective of key events in the case, including, for example, the identification of the indicated user of an electronic storage media device such as a computer or cell phone and the ability to determine when a file or e-mail was created or generated. Failure of the government to preserve and produce metadata in the appropriate case may result in drastic consequences for the prosecution, such as suppression of evidence.⁵⁷

^{54.} For example, the CFTC guidelines provide that if a document was collected from a responding person or entity in a PDF format, it can be produced in that format.

^{55.} Fed. R. Crim. P. 17(c)(1).

^{56.} Andrew Goldsmith, *Trends—Or Lack Thereof—In Criminal EDiscovery: A Pragmatic Survey of Recent Case Law*, ST036 ALI-CLE 1 (April 2012) (publication authored by U.S. Department of Justice National Criminal Discovery Coordinator).

§ 25.5 ESI Discovery Disputes, Resolution, and Remedies

With regard to ESI discovery disputes, the ESI Protocol provides that the parties must attempt to resolve ESI discovery disputes in good faith before involving the court.⁵⁸ Indeed, the ESI Protocol recommends that prosecutors and the Federal Public Defender Offices should mandate supervisory review and preapproval of all motions seeking judicial resolution of ESI discovery disputes or suggesting that opposing counsel has committed some sort of infraction involving ESI discovery.⁵⁹

As discussed earlier in this chapter, the active and specific involvement of a district court may be crucial in monitoring and policing how federal prosecutors and the agencies with which they work on a particular case handle preservation, collection, and production of e-discovery. Although the ESI Protocol's stated preference is for the parties to resolve e-discovery issues in advance of court intervention, this may not always be possible. A recent example of such a situation is set forth in recent criminal proceedings in a Kansas federal district court. In an August, 2019, decision, the chief judge of the District of Kansas issued findings of fact and conclusions of law that contained, among other things, recitations of failures by federal prosecutors to comply with e-discovery preservation and discovery requirements.⁶⁰ Among the deficiencies cited by the court in that case were: (1) failure to properly implement and monitor a litigation hold with respect to potential e-discovery; (2) failure to preserve hard drives that contained information responsive to prior court orders; (3) failure to produce emails that received "hits" on search terms previously agreed to by the government; and (4) failure to comply with orders from a magistrate judge concerning, among other things, e-discovery.⁶¹

As other examples, a district court might resolve an issue related to e-discovery by mandating that the government provide access to defense counsel of a device from which electronic evidence was taken;⁶² or alternatively finding that because a defen-

59. ESI Protocol, Recommendations, p. 5.

- 61. Carter, 2019 WL 3798142 at *15-29.
- 62. See, e.g., United States v. Reyna, 98 F.Supp.3d 895, 898 (W.D. Tex. 2015).

^{57.} Goldsmith, *Trends—Or Lack Thereof—In Criminal EDiscovery*, ST036 ALI-CLE 1 (citing, among other cases, *United States v. Cross*, No. 07-cr-730 (DLI), 2009 WL 3233267 (S.D.N.Y. Oct. 2, 2009), a case in which the district court suppressed a photo array based on the government's failure to retain and produce metadata associated with the array).

^{58.} ESI Protocol, Introduction, p. 2.

^{60.} United States v. Carter, No. 16-20032-02-JAR, 2019 WL 3798142 (D. Kan. Aug. 13, 2019), appeal dismissed, No. 19-3199, 2019 WL 8231644 (10th Cir. Dec. 5, 2019), order vacated in part, No. 16-20032-02-JAR, 2020 WL 430739 (D. Kan. Jan. 28, 2020).

dant has been provided forensic copies of the data on a device, no access to the device itself is warranted.⁶³ As another example, a court may be required to determine that discovery of the source code used by investigators to identify an online child predator is not material to the defense of the resulting charge.⁶⁴ In making decisions on production of e-discovery in criminal cases, the absence of specific provisions in the Federal Rules of Criminal Procedure presents both an opportunity and a challenge, as one district court has noted:

The problem now is that, absent a rule, each judge faced with a motion to compel criminal discovery with ESI data will have to devise his or her own scheme for ESI discovery based upon the relief sought by the parties, define what is the standard for production of that ESI material, and determine whether the producing party has satisfied the newly proclaimed standard for production and which party—the Government or defense—is to bear the costs (both in money, time, technological competence, and memory space) associated with ESI discovery.⁶⁵

§ 25.6 Brady Obligations and "Data Dumps" of ESI

An important issue relating to e-discovery is how prosecutors satisfy their duties under *Brady v. Maryland*⁶⁶—the seminal Supreme Court case on the need for the prosecution in federal or state court to disclose information and materials "favorable to an accused upon request"—in an e-discovery context involving significant amounts of data. Especially considering trends in criminal discovery over the past few decades, most federal prosecutors seek to achieve *Brady* compliance by providing voluminous electronic "open file" discovery. In *United States v. Skilling*,⁶⁷ the Fifth Circuit held that the prosecution in that case satisfied its *Brady* obligations when it gave the defense access to a database consisting of several hundred million pages of documents.⁶⁸ Noting that the prosecution generally has no duty to direct defendants to exculpatory evidence, the *Skilling* court found dispositive that the open file was electronic and searchable, that the government produced a set of "hot documents" that it

66. 373 U.S. 83 (1963).

68. Skilling, 554 F.3d at 577.

^{63.} See, e.g., United States v. Abrams, 761 F.Appx. 670, 676-77 (9th Cir. 2019).

^{64.} United States v. Jean, 891 F.3d 712, 715 (8th Cir.), cert. denied, 139 S. Ct. 440 (2018).

^{65.} United States v. Briggs, No. 10CR1845, 2011 WL 4017886, at *7 (W.D.N.Y. Sept. 8, 2011).

^{67. 554} F.3d 529 (5th Cir. 2009), affirmed in part and vacated in part on other grounds, 561 U.S. 358, 130 S. Ct. 2896 (2010).

ESI Discovery in Texas Criminal Practice

believed were important to its own case and to Skilling's defense, and that it also provided access to other Enron litigation databases.⁶⁹ Importantly, the court expressly limited its holding to the facts of the *Skilling* case, remarking that "[w]e do not hold that the use of a voluminous open file, can never violate *Brady*."⁷⁰ The Court gave examples of government conduct that could lead to a finding of a *Brady* violation through the use of an open file including padding an open file "with pointless or superfluous information to frustrate a defendant's review," creating a voluminous file that is "unduly onerous," or hiding *Brady* material of which it is aware in a huge open file in the hopes that the defendant will not locate it.⁷¹

In the years since, a number of courts have followed Skilling, including the Sixth Circuit.⁷² In *United States v. Warshak*, the Sixth Circuit declined to find a *Brady* violation on the basis of the government's provision of open file discovery consisting of millions of pages of documents.⁷³ As in *Skilling*, in *Warshak*, the Court cited to the lack of evidence of bad faith on the part of the prosecution.⁷⁴ There was no evidence that the government "larded its production with entirely irrelevant documents" or "made access to the documents unduly onerous."⁷⁵ In so doing, the appellate court rejected the defense argument that the "untenably burdensome" nature of an e-discovery production represented an "abdication" by the government of its *Brady* obligations.⁷⁶ In *Skilling, Warshak*, and the cases following them, a critical consideration is the searchability of the ESI disclosed in discovery.⁷⁷

A few courts have imposed more stringent discovery burdens on the government. For example, in *United States v. Salyer*,⁷⁸ a case involving a large volume of electronic discovery and an incarcerated defendant, a magistrate judge ordered the government

- 69. Skilling, 554 F.3d at 577.
- 70. Skilling, 554 F.3d at 577.
- 71. Skilling, 554 F.3d at 577.
- 72. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

73. 631 F.3d 266, 297–98 (6th Cir. 2010) As the defendants noted in their appellate briefing, the government produced in discovery "three tera-drives containing more than 17 *million pages* of documents." Brief of Appellants Steven Warshak, Harriet Warshak, and Tci Media, Inc., 2009 WL 1581797 (filed May 29, 2009) (emphasis in original) (hereinafter Warshak Appellants' Brief).

- 74. Warshak, 631 F.3d at 297-98.
- 75. Warshak, 631 F.3d at 297.
- 76. Warshak Appellants' Brief.

77. See, e.g., United States v. Rubin/Chambers, 825 F. Supp. 2d 451, 454–55 (S.D.N.Y. 2011) (holding no Brady violation occurred in light of the facts that the materials disclosed were searchable electronic productions and the government provided multiple indexes).

78. 271 F.R.D. 148, 158 (E.D. Cal. 2010).

to organize and identify for the defense discoverable information under Federal Rule of Criminal Procedure 16, *Brady*, and *Giglio*.⁷⁹ However, it can be argued that a case such as Salyer may be limited in application to incarcerated defendants with relatively small defense teams and limited resources.⁸⁰ *Salyer* undoubtedly has some limits, as another order in the case recognized that the court did not have authority to require the government to establish a "common data base" containing the information that would be accessible to both the government and defense.⁸¹ Nonetheless, prosecutors and defense counsel alike should be aware of the prevailing case law in the jurisdiction on whether the government can satisfy its *Brady* obligations through a "data dump," as opposed to particularized disclosures of specific information from within gigabytes or terabytes of data.⁸²

§ 25.7 Special Issues Regarding Criminal ESI

§ 25.7:1 Funding under the Federal Criminal Justice Act

Special rules apply when criminal defense counsel seeks to obtain funding for computer hardware, software, or litigation support services under the Criminal Justice Act. Appointed counsel may, of course, seek such funding if a case warrants it. Even if a defendant has retained counsel but is financially unable to obtain the necessary services, the court can authorize funding for ESI management or other expert services under the Criminal Justice Act. Under such circumstances, however, counsel must disclose his or her fee agreement to the court, and the court may order counsel to pay all or part of the expenses if the fee arrangement is unreasonable in relation to customary fees or if the fee agreement was made with a gross disregard of the defendant's anticipated trial expenses.⁸³ When funding is sought for computer hardware, software, or litigation support products or services, or for computer experts expected to cost

^{79.} Giglio v. United States, 405 U.S. 150, 92 S. Ct. 763 (1972).

^{80.} See Rubin, 825 F.Supp.2d at 456 (distinguishing Salyer on basis that defendant in Salyer was detained, had a relatively small defense team, and no access to documents from a parallel civil proceeding or access to voluntary corporate assistance to locate documents).

^{81.} United States v. Salyer, No. S-10-0061 LKK [GGH], 2011 WL 1466887, at *8-10 (E.D. Cal. Apr. 11, 2011).

^{82.} For a further discussion of the issue of "data dumps" and *Brady* obligations, see Hilary Oran, *Does Brady Have Byte? Adapting Constitutional Disclosure for the Digital Age*, 50 Colum. J.L. & Soc. Probs. 97 (2016).

^{83.} Guide to Judiciary Policy, Vol. 7(A) § 310.10.20, www.uscourts.gov/sites/default/files/vol07a -ch03.pdf.

more than \$10,000, counsel must consult with the Office of Defender Services (ODS). Moreover, counsel must inform the court of ODS's advice and recommendation.⁸⁴

§ 25.7:2 Confidential, Privileged, and Classified Information

Certain types of information require special handling. These can include grand jury material, documents that provide witness identification information, materials subject to protective orders, privileged documents, classified information, and so on.⁸⁵ The ESI Protocol provides that the parties have an obligation to protect such information. The duty to protect such information is magnified in the ESI context because of the ease of dissemination of electronic data.⁸⁶ The ESI Protocol requires parties to limit disclosure of potentially protected data and take reasonable measures to protect the data. The ESI Protocol also provides that in the initial discovery planning meeting, the parties should discuss potential issues relating to sensitive data and take steps to prevent unauthorized disclosure of such information, possibly including seeking a protective order from the court.⁸⁷

§ 25.7:3 Non-Releasable Discovery

In certain cases ESI is itself contraband and non-releasable to the defense. An example is child pornography.⁸⁸ In such cases the prosecution generally requires that the ESI remain on premises, and it is generally necessary to retain an expert to perform an on-site analysis and review of the ESI. In any event, the parties should anticipate and address issues relating to contraband ESI at the initial planning meeting under the ESI Protocol and the new provision of the Federal Rules of Criminal Procedure.⁸⁹

§ 25.7:4 Metadata

The issue of metadata can be an important component of discovery in a criminal case. Metadata "can describe how, when, and by whom ESI was created, accessed, modified, formatted, or collected."⁹⁰ Examples of metadata types include data that may

88. See, e.g., United States v. Mitchell, 725 F. Appx. 544, 545 (9th Cir. 2018) (citing Adam Walsh Child Protection and Safety Act, 18 U.S.C. § 3509(m)); see also ESI Protocol, Recommendations, p. 2.

89. ESI Protocol, Recommendations, at 2.

^{84.} Guide to Judiciary Policy, Vol. 7(A) § 320.70.40.

^{85.} ESI Protocol, Recommendations, p. 5.

^{86.} ESI Protocol, Recommendations, at 5.

^{87.} ESI Protocol, Recommendations, at 5.

reflect the username associated with a word-processing document, date created, the last date it was accessed, and the sender, recipients, and transmittal information for an e-mail. Retaining the metadata associated with a document allows the parties to sort, filter, and categorize documents. Sorting, filtering, and categorizing documents using metadata can provide significant information that is not available when a document is merely text searchable. For example, e-mail files with retained metadata permit a reviewer to identify with ease e-mails sent on the same date as a target e-mail or involving the same recipient or subject. The ESI Protocol advises the parties to discuss and attempt to resolve questions regarding the treatment of metadata in ESI productions, including questions surrounding metadata in third-party ESI, in native files, and in ESI converted to electronic image formats.⁹¹

§ 25.7:5 Detained Clients

Unlike in the civil arena, in a criminal case, a criminal defendant may be detained pending trial. This circumstance creates unique issues for counsel. In a case involving large volumes of electronic discovery, the sheer volume of data involved may make it impossible for an incarcerated defendant to review discovery in paper form. In such circumstances, it is important for defense counsel to address these discovery access issues both with the prosecution and with the court in order to ensure that the defendant can provide meaningful assistance to his lawyer in preparing a defense.⁹² Because of the wide variations in rules, security needs, and resources among detention facilities, the ESI Protocol does not announce uniform rules governing providing detained clients with access to ESI.⁹³

§ 25.8 State Criminal Discovery Rules and ESI

Texas state criminal law has historically—to put it charitably—been noticeably undeveloped in the area of ESI discovery. This relates in part to several factors. First, the reality is that for decades in Texas, most prosecutor offices around the state were decidedly low-tech operations, and many (especially in rural jurisdictions) continue to be so. Second, given the nature of their day-to-day workload, few state prosecutor offices have dealt routinely with cases involving large amounts of ESI, as opposed to cases that might involve at most one or several video or audio files of traffic stops,

- 91. ESI Protocol, Strategies, pp. 4-5, 8.
- 92. ESI Protocol, Strategies, p. 3.
- 93. ESI Protocol, Strategies, at 3.

^{90.} ESI Protocol, Strategies, p. 13.

reports of investigation, witness interviews, or defendant statements. Furthermore, on the "discovery" side of the ESI discovery equation, many prosecutors' offices in Texas operated for years under "closed file" policies, as they were allowed to do under the Texas Code of Criminal Procedure.⁹⁴ With such "closed file" policies, the ultimate ability of courts to order production of any "documents" to the defense was limited—even in hard copy, much less in electronic formats more familiar to civil cases.⁹⁵ Whether to allow such discovery, therefore, was historically subject to the discretion of a particular prosecutor's office.

In more recent years, most of the more than 330 state prosecutor offices around the state have adopted some form of "open file" policy under which defense counsel can inspect, copy, and/or download discovery of such prosecution file material as arrest warrant affidavits and offense reports.³⁶ However, even in those prosecutors' offices that provide access to electronic copying of case file material, the concept of adopting office-wide procedures specific to ESI—for example, procedures not only for discovery of offense reports in electronic readable format, or the viewing or copying of audio or video files of traffic stops or statements in computer-playable format, but also procedures covering inspection, review, and/or copying of electronic evidence captured by law enforcement from computer hard drives or cell phones—was slow to take hold. In the years since the Texas legislature passed the landmark Michael Morton Act, and its reforms to the criminal discovery process, many state prosecution offices—most notably those in major metropolitan areas—have rolled out technology platforms that allow defense counsel to access e-discovery in a particular case in the comfort of their office.

As state prosecutor practices with respect to ESI continue to evolve, there are an increasing number of provisions of the Texas Penal Code that explicitly involve underlying electronic data issues, such as the following:

^{94.} Texas District and County Attorneys Association, Setting the Record Straight on Prosecutorial Misconduct (2012), p.14, www.tdcaa.com/wp-content/uploads/Brady_Resources/Reports_&_Articles/Setting-the-Record-Straight.pdf (hereinafter "Setting the Record Straight") (noting that there are "no statistics available on open-file policies through time, only anecdotal evidence that many jurisdictions did not adopt open-file policies until th \geq 1990s").

^{95.} See, e.g., In re State of Texas, 162 S.W.3d 672 (Tex. App.—El Paso 2005, no pet.); In re Simmons, 799 S.W.2d 426 (Tex. App.—El Paso 1990, no pet.).

^{96.} See, e.g., Tarrant County Open File Discovery Matrix, www.tccdla.com Travis County District Attorney's Office Discovery Policy—Criminal Cases, www.traviscountytx.gov/district-attorney.

- Fraudulent use or possession of identifying information (Tex. Penal Code § 32.51): the statute was enacted in 1999 and amended in 2003 to include within its scope the possession or use of bank account numbers.⁹⁷
- Breach of computer security (Tex. Penal Code § 33.02): the statute was added to the Penal Code in 1985 to cover computer "hacking," and has been amended several times, most recently in 2011.⁹⁸
- Online solicitation of a minor (Tex. Penal Code § 33.021): The statute was added in 2005 to cover sexually explicit communications and online sexual solicitations.⁹⁹
- Online impersonation (Tex. Penal Code § 33.07): The statute was added in 2009 to cover situations in which a person uses the name or persona of another person online, including on social networking sites.
- Possession or promotion of child pornography (Tex. Penal Code § 43.26): the statute was amended in 1997 to include images displayed on a computer.¹⁰⁰
- Electronic transmission of certain visual material depicting minor (Tex. Penal Code § 43.261): the statute was enacted in 2011 to cover "sexting" activity involved in texting or other electronic transmission of a minor engaging in sexual conduct.

Furthermore, state and local law enforcement agencies have become increasingly sophisticated in terms of capacity to locate, collect, and analyze electronic data. Electronic storage media devices and data have now become commonplace components for search warrants, not only in computer-related crime investigations but also in drug, financial crime, and organized crime investigations.¹⁰¹ Given the number of federal and state joint law enforcement task forces, it is increasingly commonplace that

^{97.} See Acts 2003, 78th Leg., R.S., ch. 1104 § 4 (H.B. 2248), eff. Sept. 1, 2003. Tex. H.B. 2248, 78th Leg. (2003).

^{98.} See Acts 2011, 82d Leg., R.S., ch. 1044 § 2 (H.B. 3396), eff. Sept. 1, 2011. Tex. H.B. 3396, 82nd Leg. (2011).

^{99.} In a 2013 decision, the Court of Criminal Appeals found a portion of this statute unconstitutional. *Ex parte Lo*, 424 S.W.3d 10 (Tex. Crim. App. 2013). The statute was subsequently amended by the Texas legislature.

^{100.} Porter v. State, 996 S.W.2d 317 (Tex. App.—Austin 1999), opinion supplemented, 65 S.W.3d 72 (Tex. App.—Austin 1999).

^{101.} See, e.g., Emack v. State, 354 S.W.3d 828 (Tex. App.—Austin 2011, no pet.) (discussing search warrants executed at ranch compound related to investigation of sexual assault of children); Lown v. State, 172 S.W.3d 754 (Tex. App.—Houston [14th Dist.] 2005, no pet.) (computer disks seized as part of theft case).

state and federal law enforcement agencies collect some form of ESI as part of investigations, and this evidence may be discoverable in resulting prosecutions. As more state and local law enforcement officers collect devices and data in an ever-increasing array of criminal investigations, and as more criminal charges directly involve collection and presentation to judges and juries of electronic evidence, increased examination by courts and prosecutors' offices of best practices for discovery of such evidence by criminal defense counsel will be inevitable.

In the meantime, however, the ESI discovery practices that exist in Texas state criminal practice are (1) currently evolving electronic platforms for the downloading of such items as arrest warrants and affidavits, offense reports, and defendant statements; and (2) practices on the disclosure and/or inspection of ESI that individual prosecutors (or specialized units within larger prosecutor offices) have formulated on their own.

§ 25.8:1 Basic Texas Criminal Discovery Statute—Texas Code of Criminal Procedure Article 39.14

For decades, the Texas state criminal code did not even appear to recognize that ESI existed. The base Texas criminal discovery statute, article 39.14 of the Texas Code of Criminal Procedure, was enacted in 1965, and was left largely unchanged by the legislature until recent years. As recently as 2005, that statute provided a trial court with abundant discretion with respect to discovery by a criminal defendant of "designated documents, papers, written statements of the defendant (except written statements of witnesses and except the work product of counsel in the case and their investigators and their notes or report), books, accounts, letters, photographs, objects or tangible things not privileged, which constitute or contain evidence material to any matter involved in the action and which are in the possession, custody or control of the State or any of its agencies."¹⁰²

It was not until 2005 that the legislature somewhat curtailed a trial court's "may allow" discretion, providing that a trial court "shall allow" discovery of the items enumerated in the Code if the defendant "show[ed] good cause therefor."¹⁰³ Of course, a trial court retained discretion even after that amendment to determine what constituted "good cause" for requested discovery.

^{102.} Acts 2005, 79th Leg., R.S., ch. 1019, § 1 (H.B. 969), eff. June 18, 2005. Tex. H.B. 969, 79th Leg. (2005).

^{103.} Acts 2005, 79th Leg., R.S., ch. 1019, § 1 (H.B. 969), eff. June 18, 2005.

The Texas Code of Criminal Procedure finally made its first explicit reference to electronic discovery in 2013, when the discovery statute, with its references to documents, papers, writings, and "tangible things," was updated (effective as of January 1, 2014) through the Michael Morton Act.¹⁰⁴ This update imposed mandatory discovery obligations on the state (upon a timely discovery request from the defendant) by eliminating the requirement of showing "good cause" for discovery to a trial court. Also, for the first time, the Code now refers to the "electronic duplication" of such items as offense reports, recorded statements of witnesses, and evidence in the possession of the state¹⁰⁵—marking the first time the concept of "electronic" discovery became an explicit part of the Code. Furthermore, the revised statute requires prosecutors to make an electronic record or other documentation of all discovery provided in a case and also requires prosecutors and defense counsel to document, as part of pleas or trials, the discovery that has been provided in a case.¹⁰⁶

However, it is important to note that even now, and with the 2013 amendments, the state criminal discovery statute does not make any explicit reference to electronic data as a specific component of "evidence material" to a criminal matter for which the state has mandatory production obligations. The current statute also does not set out any particular remedy for instances of noncompliance with discovery obligations under the statute by the state.¹⁰⁷ However, there is no doubt that the statute as revised does give a criminal defense attorney a stronger basis on which to argue that the state's basic discovery obligations may extend to data in the state's possession. After all, any data in the state's possession likely came from one or more "objects" or "tangible things" in the state's possession, such as a hard drive or thumb drive.¹⁰⁸ Accordingly, criminal defense counsel should include in a motion for discovery, under article 39.14 and constitutional discovery principles, requests for electronic data and ESI that is in the possession of the state, including in the possession of law enforcement agencies involved in the investigation leading to the case.

When this book was originally published, online e-discovery platforms were in their infancy. Since that time, several prosecutors' offices around the state have taken extensive and expensive steps to both modernize and streamline the delivery of discovery to defense counsel through electronic platforms, the most prevalent of which is

^{104.} Acts 2013, 83d Leg., R.S., ch. 49, § 2 (S.B. 1611), eff. Jan. 1, 2014. Tex. S.B. 1611, 83rd Leg. (2013).

^{105.} Tex. R. Crim. P. 39.14(b) (eff. Jan. 1, 2014).

^{106.} Tex. Code Crim. Proc. art. 39.14(b), (i), (j).

^{107.} Tex. Code Crim. Proc. art. 39.14(b), (i), (j).

^{108.} See, e.g., Miller v. State, 335 S.W.3d 847 (Tex. App.-Austin 2011, no pet.).
ESI Discovery in Texas Criminal Practice

named "TechShare." These electronic platforms have the capability of allowing authorized defense counsel who have made an appearance in a case to log in through portals and access case information in PDF format, such as arrest warrants, affidavits, and offense reports. The platforms also allow authorized defense counsel to download such written materials and review videos and audio recordings relevant to a case.¹⁰⁹ These video and audio materials can be downloaded in native format, which may be important when reviewing any metadata associated with them. These platforms sometimes also include a notification system that sends e-mails to defense counsel of initial and supplemental material made available through the platform.

These electronic platforms have evolved to handle ESI discovery practices and requirements in most cases brought by a state prosecutor in the offices that use such a platform. However, there are exceptions. First, many prosecutors' offices allow some form of precharge discovery in cases, such as white-collar investigations, that commonly involve ESI, and the electronic platforms will contain disclosures that begin with a charge, through a returned indictment or a filed information. Second, even when fully implemented, these platforms may not have the capability to handle every large data set, such as a forensic download of cell phone data or a forensic image of a computer. Such larger productions of ESI in a format amenable to forensic review of the underlying ESI will be made on electronic storage media, such as hard drives or thumb drives. As the e-discovery platforms have evolved, state prosecutor offices have revised their office discovery policies and continue to evaluate continued revisions to take ESI and its discovery, through an online platform or through other means, into account.

Another consequence of the advent of electronic discovery platforms has been the need for many criminal defense practitioners to upgrade their computer hardware and Internet service. The processing speed of a computer used to access e-discovery platform is obviously critical to how quickly that material can be downloaded and reviewed. Likewise, some forms of e-discovery (such as certain videos) may be in a native format that requires a particular form of viewing software. When e-discovery platforms first came online, many criminal defense practitioners complained about an inability to access materials or overly slow download times on such things as dashcam or bodycam videos. In many instances these were not issues with the platforms but with the outdated computer systems and slow Internet access used by criminal

^{109.} Many urban counties—such as Bexar, Dallas, Harris, and Travis—worked with the Texas Conference of Urban Counties to implement the TechShare case management system that includes a "Prosecutor Defense Attorney Portal" through which case materials may be shared electronically. Information on the development of the TechShare platform can be found at https://techsharetx.gov/.

defense counsel instead. So criminal defense practitioners have also had to evolve their working practices and office equipment to keep up with the times.

§ 25.8:2 ESI Discovery and "Data Dumps" in Texas Criminal Cases

As mentioned previously, upon timely request by a defendant, the Michael Morton Act requires the state to produce certain evidence to the defense. Tex. Code Crim. Proc. article 39.14(a) requires that the state produce evidence "material to any matter involved in the action and that are in possession, custody, or control of the state or any person under contract with the state." There is no doubt that the Michael Morton Act "amended and enlarged article 39.14 of the code of criminal procedure relating to the State's duty to provide discovery to criminal defendants."¹⁰ When examining the implications of this statute, it is important to note that civil and criminal discovery serve very different purposes. There are significantly higher stakes present in criminal cases, and the discovery rules reflect this difference because one of the main goals of criminal law is the protection of a defendant's constitutional rights. Unlike in civil cases in which the rules of procedure promote a level playing field and equal access to evidence, the Texas rules of criminal procedure seek to ensure that a defendant receives a fair trial, including the ability to fully encounter (and challenge) the state's case through discovery, including ESI discovery.

The same issues of "data dumps" occur in the state criminal e-discovery context as in federal cases. With ESI, state prosecutors can "dump" voluminous amounts of data on the defense and then argue that they complied with *Brady* and current case law by making it available. This presents an obvious challenge for any defendant or defense practitioner, especially for those indigent defendants with court-appointed attorneys who do not have the time or resources to review and analyze all the data. For example, the state can produce lengthy sections of dashcam or bodycam recordings, or hundreds of recorded jail calls made by the defendant that can amount to hundreds of hours of video and/or audio recording, the majority of which has no relevance to the case. In other instances, the state can turn over voluminous ESI shortly before the trial, making it impossible for the defense to find the favorable or damning evidence. Finally, the state can produce ESI in a format that requires expensive, proprietary software and outside ESI vendors to properly load and review.

^{110.} Cervantez v. State, No. 02-16-00224-CR, 2018 WL 5289458, at *2 (Tex. App.—Fort Worth Oct. 25, 2018, pet. ref'd).

In 2016, a Texas court decided In re State ex rel. Skurka,¹¹¹ a case involving an indictment of a defendant for aggravated assault as a habitual felony offender and assault family violence with a prior conviction.¹¹² During the course of that case, the state discovered and produced recordings of more than one thousand telephone calls made by the defendant while he was incarcerated.¹¹³ The trial court ultimately ordered pretrial disclosure of the specific jailhouse telephone recordings of the defendant that the state intended to use at trial and the state petitioned for writ of mandamus.¹¹⁴ The state argued that the trial court's order was an abuse of discretion for several reasons. including: (i) it required the state to create a document that did not exist because they had to create a list of jail recording it intended to use, and (ii) it violated the work product privilege because disclosing this information would require them disclosing information about their mental process and trial strategy.¹¹⁵ The Corpus Christi Court of Appeals denied the state's petition and, among other things, held that (i) the trial court's order did not improperly require the state to create discovery materials not within its possession, custody, or control; and that (ii) the order did not violate the work product doctrine.¹¹⁶ Cases like Skurka support the proposition that the state may be required in the appropriate case to at least generally specify the ESI data they intend to use in their case in chief, while respecting the legal and ethical requirements to make "full" discovery in criminal cases.

§ 25.8:3 Prosecutorial Misconduct

Of course, prosecutors must be ever mindful that ESI discovery, if not properly handled and disclosed, can lead to attorney grievances and findings. For example, the Texas Board of Disciplinary Appeals illustrated how to apply the Texas Disciplinary Rules of Professional Conduct, in the context of discovery, in its decision *Schultz v. Commission for Lawyer Discipline*.¹¹⁷

Rule 3.09(d), entitled "Special Responsibilities of a Prosecutor," states the prosecutor in a criminal case shall:

^{111. 512} S.W.3d 444 (Tex. App.-Corpus Christi-Edinburg June 13, 2016, no pet.).

^{112.} In re State ex rel. Skurka, 512 S.W.3d at 447-50.

^{113.} In re State ex rel. Skurka, 512 S.W.3d at 447-50.

^{114.} In re State ex rel. Skurka, 512 S.W.3d at 447-50.

^{115.} In re State ex rel. Skurka, 512 S.W.3d at 447-50.

^{116.} In re State ex rel. Skurka, 512 S.W.3d at 451-56.

^{117.} No. D0121247202, 2015 WL 9855916 (Texas Bd. Disp. App. 55649, Dec. 17, 2015, no appeal).

[M]ake timely disclosure to the defense of all evidence or information known to the prosecutor that tends to negate the guilt of the accused or mitigates the offense . . . except when the prosecutor is relieved of this responsibility by a protective order of the tribunal¹¹⁸

Schultz reviewed an aggravated assault case prosecuted by state prosecutor.¹¹⁹ In that case, the complaining witness suspected her estranged husband as the perpetrator of her attack, on the basis of her alleged attacker's smell and stature, rather than through positive visual identification.¹²⁰ The complaining witness told police and testified in a hearing that her husband attacked her without revealing she failed to see her husband.¹²¹ The prosecutor met with the complaining witness one month before trial, and the witness explained for the first time that she never saw her husband's face during her attack because of the dim lighting in the room.¹²² The prosecutor did not reveal the information to defense counsel, but rather the information came out when the complaining witness testified at trial, including the fact that she previously told the prosecutor about the lack of positive identification.¹²³ Defense counsel sought and was granted a mistrial, and then filed a grievance against Schultz.¹²⁴

The prosecutor argued for the Board of Disciplinary Appeals to interpret rule 3.09(d) under the *Brady* materiality standard, asserting the evidence he failed to disclose was neither material nor exculpatory.¹²⁵ The board quotes *Brady*'s holding that "suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution."¹²⁶ Evidence is material "if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different."¹²⁷ While *Brady* ensures the criminal defendant his right to a fair trial, the board explained that "the ethics rule and disciplinary proceedings serve an entirely different purpose: protection of the public."¹²⁸

118. Tex. Disciplinary Rules Prof'l Conduct R. 3.09(d).

- 120. Schultz, 2015 WL 9855916, at *3.
- 121. Schultz, 2015 WL 9855916, at *4.
- 122. Schultz, 2015 WL 9855916, at *5.
- 123. Schultz, 2015 WL 9855916, at *5.
- 124. Schultz, 2015 WL 9855916, at *6-7.
- 125. Schultz, 2015 WL 9855916, at *2.

- 127. Kyles v. Whitley, 514 U.S. 419, 433 (1995).
- 128. Schultz, 2015 WL 9855916, at *7.

^{119.} Schultz, 2015 WL 9855916, at *2.

^{126.} Schultz, 2015 WL 9855916, at *6; see also Brady v. Maryland, 373 U.S. 83, 87 (1963).

Brady's materiality standard makes little sense "in the context of an aborted prosecution" due to necessary speculation.¹²⁹ To limit prosecutor accountability only to cases which result in conviction "would limit prosecutors' accountability to the public" the very reason for the existence of an ethical duty.¹³⁰

The board described the "unambiguous" nature of rule 3.09(d) as follows:

The goal of rule 3.09(d) is to impose on a prosecutor a professional obligation to "see that the defendant is accorded procedural justice, that the defendant's guilt is decided upon the basis of sufficient evidence, and that any sentence imposed is based on all unprivileged information known to the prosecutor." Tex. Disciplinary Rules Prof'l Conduct R. 3.09(d) cmt. 1.

. . . .

Ethically, under rule 3.09(d) the prosecution must turn over any information that "tends to negate the guilt" or mitigate the offense. There is no materiality requirement. No analysis is necessary to determine whether disclosure would probably have led to a different outcome of the trial. The information need not be admissible at trial, and the information must be disclosed "timely," that is, "as soon as reasonably practicable so that the defense can make meaningful use of it." ABA Formal Op. 09-454.

. . . .

The ethics rules acknowledge that a prosecutor shall not make a determination of materiality in his ethical obligation to disclose information to the defense....Rule 3.09(d) is specifically intended to advise—and prevent a prosecutor from making an incorrect judgment call, such as that Maria's "inconsistent statements" did not rise to the level of *Brady*-mandated disclosure. The clarity of rule 3.09(d) is a safeguard for prosecutors and citizens alike: if there is any way a piece of information could be viewed as exculpatory, impeaching, or mitigating—err on the side of disclosure.¹³¹

Schultz reiterates the holding in *Giglic v. United States*, 405 U.S. 150, 92 S. Ct. 763 (1972) that "*Brady* applies equally to evidence relevant to the credibility of a key witness in the state's case against a defendant."¹³² The board ultimately found substantial

^{129.} Schultz, 2015 WL 9855916, at *7.

^{130.} Schultz, 2015 WL 9855916, at *7.

^{131.} Schultz, 2015 WL 9855916, at *6 (emphasis added).

^{132.} Schultz, 2015 WL 9855916, at *7 (quoting Graves v. Dretke, 442 F.3d 334, 339 (5th Cir. 2006)).

evidence that "(1) [the prosecutor] had actual knowledge that the state's key witness could not identify her attacker directly and that he failed to disclose it to the defense."¹³³ While rule 3.09(d) "limits the information to that actually known by the prosecutor, . . . actual knowledge may be inferred from circumstances."¹³⁴ Additionally, although not necessary to prove a violation of rule 3.09(d), the board affirmed that "(2) [the prosecutor's] failure to disclose the limited nature of the witness's ability to identify her attacker constituted material evidence under *Brady*."¹³⁵

The board also addressed rule 3.04(a), entitled "Fairness in Adjudicatory Proceedings," which states a "lawyer shall not unlawfully obstruct another party's access to evidence; in anticipation of a dispute unlawfully alter, destroy or conceal a document or other material that a competent lawyer would believe has potential or actual evidentiary value."¹³⁶ The board rejected the prosecutor's contention that rule 3.04(a) requires intent, holding instead that the rule applies "to the situation where a prosecutor failed to disclose information tending to negate the guilt of the accused as required by rule 3.09(d) or other law, regardless of intent."¹³⁷ The board noted, "[b]y misrepresenting that he had provided full discovery, [the prosecutor] perpetuated the defense's mistaken belief that it had received all exculpatory evidence."¹³⁸

Although the *Schultz* decision dealt with failure to disclose exculpatory evidence disclosed orally by a complaining witness, its potential application to situations involving e-discovery are readily apparent. Under the principles discussed in *Schultz*, it remains a very perilous exercise for a prosecutor to make a subjective judgment as to what ESI has potential or actual evidentiary value. This is especially true when theories of defense are within the purview of criminal defense counsel, and not prosecutors. It is for this reason that many prosecutor offices across the state have adopted "open file" policies.

§ 25.8:4 Discovery of Child Pornography Images

The Texas Legislature enacted changes to the Code of Criminal Procedure in 2009, in response to the burgeoning number of child pornography and abuse image cases being

- 133. Schultz, 2015 WL 9855916, at *12.
- 134. Schultz, 2015 WL 9855916, at *6.
- 135. Schultz, 2015 WL 9855916, at *6.
- 136. Schultz, 2015 WL 9855916, at *9.
- 137. Schultz, 2015 WL 9855916, at *9.
- 138. Schultz, 2015 WL 9855916, at *12.

§ 25.8

investigated and prosecuted in the state.¹³⁹ At that time, the legislature specifically addressed discovery by defendants and defense counsel of child pornography images, either in hard-copy or digital format. Under this provision, no copying or further distribution of these images is allowed in discovery. Instead, appropriate discovery of such material is made if "the state provides ample opportunity for the inspection, viewing, and examination of the property or material" by the defendant and his counsel and forensic expert.¹⁴⁰

§ 25.8:5 Discovery of Child Abuse Evidence and Forensic Interview or Recorded Statement of a Child

The legislature further amended Texas Code of Criminal Procedure article 39.15 in 2011 to include material covered by the newly enacted "sexting" statute and also forensic interviews of children and statements taken from children in cases of alleged abuse.¹⁴¹ Thus, these "sexting" materials and recorded forensic interviews of children are also explicitly excluded from the scope of electronic discovery material that may be "copied" to defense counsel. Instead, these materials may only be inspected, viewed, and examined in the same manner as child pornography as part of the discovery process. If a state prosecutor office has an online platform for disclosure and downloading discovery, these materials (like child pornography images) are not placed into that system. For these materials, defense counsel must still go to the prosecutor's office to review.

§ 25.8:6 Case-Specific State Criminal ESI Protocols

In the appropriate case, prosecutors and defendants can and do negotiate—and seek court intervention and rulings as necessary—formal or informal protocols for the inspection of ESI by the defense, and/or the provision of a copy of ESI to the defense. In some cases, a prosecutor's office may be willing to provide a copy of ESI to defense counsel without any protocol, as part of an "open file" policy. Others may require a written protocol. Whether written or unwritten, such protocols and agree-

^{139.} Tex. Code Crim. P. art. 39.15.

^{140.} See In re State, 564 S.W.3d 58, 64–66 (Tex. App.—El Paso 2018) (orig. proceeding) (reversing trial court order to state to copy images of child pornography and provide to the defense).

^{141.} This change was in response to *In re District Attorney's Office of the 25th Judicial District*, 358 S.W.3d 244 (Tex. Crim. App. 2011), in which the Texas Court of Criminal Appeals held that under article 39.14, a trial court could order the copying of a forensic interview of a child by the state to defense counsel.

ments can cover the topics below, depending on the case and its particular circumstances.

Will a copy of the ESI be made available, or will the data be available for review only in a prosecutor's office or on a law enforcement computer? The issue of whether a court can and should order the state to provide a copy of ESI to the defense, as opposed to providing the data for inspection on a law enforcement computer, is an open question. At least one court has found, under circumstances giving rise to a suggestion that the ESI might contain exculpatory information about whether images of claimed child pornography could be properly tied back to the defendant's computer, that the state should have provided a copy to the defense to analyze on their own, using their own equipment.¹⁴² However, other cases have found that the state's offer to the defense to inspect the data at a law enforcement forensics lab, under the supervision of law enforcement authorities, satisfies the state's discovery obligations.¹⁴³ As indicated above, some materials (such as child pornography images) cannot by statute be made available as a copy to defense counsel. With these exceptions, however, providing a copy of ESI to defense counsel may be a method that satisfies a number of concerns for the prosecutor's office, including avoiding potential claims of prosecutorial misconduct and avoiding additional discovery burdens on law enforcement agencies involved in a case.

If the ESI is only made available for inspection, what types of searches by defense experts can be done during the inspection? If the state is only permitting "inspection" access on equipment owned and controlled by law enforcement, will the platform on which the ESI is made available allow defense counsel (or more likely a forensic expert retained by defense counsel) to do searches across the data, such as keyword or date searches?

If a copy of all ESI is not being delivered to defense counsel for examination by defense forensic experts, can defense counsel submit search terms to the state

^{142.} In *Taylor v. State*, 93 S.W.3d 487 (Tex. App.—Texarkana 2002, pet. ref'd), the appellate court held: "We would not require a chemist to take a 'porta-lab' with him or her into an evidence room to check alleged contraband drugs, and it is not appropriate to require a computer expert to carry his or her equipment into a State facility to review the documents. Under some circumstances, such as in this case where the accuracy of the copy itself is at issue, on timely request the duplicate and the original hard drive should both be produced for independent examination."

^{143.} Even before the Texas Code of Criminal Procedure was amended to prohibit copying of child pornographic images, these courts found that the state's offer to have the defense inspect the images at a law enforcement facility was sufficient discovery; *see Savage v. State*, Nos. 05-06-00174-CR, 05-06-00175-CR, 2008 WL 726229 (Tex. App.—Dallas Mar. 19, 2008, pet. ref'd); *see also Rogers v. State*, 113 S.W.3d 452 (Tex. App.—San Antonio 2003, no pet.).

and obtain copies of data responsive to those searches? Even if the state will not agree to (and a court will not order) the production of all ESI on a case, a potential middle ground is to allow the defense to have law enforcement authorities run searches across the data, such as keyword or date searches, and have that resulting data produced.

If a copy of the ESI is being made available for inspection or delivered to defense counsel, in what format will the ESI be delivered? Will the defense receive forensic images of individual storage devices or a collection of data taken from multiple sources? This question will likely require most defense attorneys to consult a forensic consultant or expert. Understanding the format in which the data is being delivered is crucial, as well as understanding what document review software will allow the user to read the data. A forensic image is a forensic copy (sometimes called a "mirror image") of a particular piece of storage media, such as a computer's hard drive. Forensic experts have access to several commercial software programs that will allow them to access these forensic images.¹⁴⁴

If the delivered or inspected data is not strictly one or more forensic images of identified electronic media storage devices, and a consolidated set of data is being produced, will the data be provided in native format? Native format is the data file format (such as JPEG files for photos, DOC or DOCX files for word processing documents, XLS for spreadsheets, HTML files for Internet search materials, or PST files for e-mail) used to initially create, edit, or publish the data. Production of data in native format may allow a forensic examiner not only to review the data in the format in which it was created but also to look for metadata, such as information about when the document was created, edited, or loaded into the device from which it was retrieved.¹⁴⁵ It will also allow a forensic examiner to look for file path information, such as whether the data was in an active or cached file and the username employed in creating or editing the data.¹⁴⁶

^{144.} Prosecutors and defense counsel working on cases involving ESI will often see or hear about references to EnCase or I-Look software, which is a common software applied in the examination of forensic images. For examples, see *Krause v. State*, 243 S.W.3d 95 (Tex. App.—Houston [1st Dist. 2007, pet. ref'd), and *Zaratti v. State*, No. 01-04-01019-CR, 2006 WL 2506899 (Tex. App.—Houston [1st Dist.] Aug. 31, 2006, pet. ref'd).

^{145.} See, e.g., McKissick v. State, 209 S.W.3d 205 (Tex. App.—Houston [1st Dist.] 2006, pet. ref'd) (describing download of photos onto computer).

^{146.} For examples of why this information might be important, see Assousa v. State, No. 05-08-00007-CR, 2009 WL 1416759 (Tex. App.—Dallas May 21, 2009, pet. ref'd), and Perry v. State, No. 2-06-378-CR, 2008 WL 3877303 (Tex. App.—Fort Worth Aug. 21, 2008, pet. ref'd).

If consolidated data from several electronic media storage devices is being delivered, how will the data be organized, or "foldered," or otherwise electronically labeled to allow a reviewer of the data to tie particular data back to a particular media storage device? If consolidated data is being delivered, it will be important to be able to tie data "sets" back to particular devices. This may be crucial to a full examination of the state's evidence and the state's ability to tie data, or access to data, back to a particular individual.¹⁴⁷ This is especially true in cases involving seizures of data not only from multiple electronic media storage devices but also from multiple rooms in one building or from multiple buildings.

Depending on the volume of the ESI, what device (such as a hard drive) with what storage capacity should the defense deliver to the prosecutor's office for the download of the data? Prosecutors will sometimes require defense counsel to deliver electronic storage media (such as an external hard drive) to the prosecutor's office or to law enforcement for use in downloading the defense's copy of ESI. To avoid issues, prosecutors will often require the electronic media storage device to be "clean" and not previously used.

Who will have access to the copy of the ESI made available by the prosecutor's office? A protocol will often specify whether access to ESI (either inspection access or access through delivery of a copy of ESI) will be restricted to defense counsel, defense counsel staff, and hired forensic experts, or whether the defendant will also have direct access to the data. More recent amendments to the base Texas criminal discovery rule make clear that a defendant can have access to discovery provided, with witness identifying information (such as address, telephone number, and Social Security number information) redacted. A defendant will not be entitled to copies of the discovery, with the exception of the defendant's own statement.¹⁴⁸ As one court has indicated:

Despite these statutory allusions to "the defendant," however, when read as a whole, the statute does not literally contemplate that a defendant should be able to personally retain a duplicate or copy of any of this discovery material (other than his own witness statement)—at least not if he is represented by counsel.¹⁴⁹

^{147.} For an example of how a piece of data can be tied back to a particular user and file path on a computer, see *Gant v. State*, 278 S.W.3d 836 (Tex. App.—Houston [14th Dist.] 2009, no pet.).

^{148.} Tex. Code Crim. Proc. art. 39.14(f) (eff. Jan. 1, 2014).

^{149.} Powell v. Hocker, 516 S.W.3d 488, 495 (Tex. Crim. App. 2017).

How will any of the data be filed with the court? A protocol may specify whether data provided through the protocol should be filed with a court, so as to avoid any of the restrictions on public disclosure of personal identifying information and the like. Many jurisdictions already have standing orders related to redaction of personal identifying information from materials filed, through e-filing or otherwise, with the courts.

What will the procedure be for the defense to make claims of privilege with respect to ESI material provided? If in the case of a search (e.g., of a lawyer's office) that may have resulted in law enforcement obtaining data that might be privileged, defense counsel may have already negotiated with a prosecutor's office, or had a court order, for review of seized material by a "taint team"—that is, a team of law enforcement officers and lawyers not involved in the case who can review the seized material for potential privilege and not be tainted by exposure to that privileged information. Even if a taint review protocol or order has been entered, however, the discovery protocol may provide what is called in the civil context a snapback provision.¹⁵⁰ Such a snapback provision in an ESI discovery protocol would allow defense counsel to identify data that defense counsel believes is privileged and have that material segmented for additional review by a taint team or by the court.

§ 25.8:7 Arguments for Increased Access to ESI Discovery

As previously discussed with respect to federal courts—especially following the 2019 amendment to the Federal Rules of Criminal Procedure—Texas state courts may be increasingly faced with discovery motions from defendants that explicitly call for the discovery of ESI. As with all discovery matters, courts are likely to rely on prosecutors and defense counsel to confer and agree if possible on the scope of all discovery, including ESI discovery. If defense counsel cannot come to a reasonable agreement with a state prosecutor's office over ESI discovery, the following arguments among others may come into play before courts hearing article 39.14 discovery motions:

1. As indicated earlier in the chapter, the state will often seek to authenticate a piece of electronic evidence, through a forensic examiner or other witness, by describing how it was obtained from a particular electronic media storage device.¹⁵¹ In such a case, a defendant can argue that without independent access to the ESI, in native format, the defendant has no meaningful method of testing the accuracy of that testimony.

^{150.} Tex. R. Civ. P. 193.3(d).

^{151.} See, e.g., Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012) (authentication of MySpace pages through lay witness).

- 2. As indicated earlier in the chapter, the state will often seek to have forensic experts or other witnesses testify as to the source and/or metadata associated with a particular file, such as an e-mail, word-processing document, photograph, or web page.¹⁵² Again, an argument can be made that without independent access to the ESI, in native format, a defendant has no meaningful method of testing the accuracy of that testimony.
- 3. Prosecutors must be increasingly wary of their obligations to produce exculpatory and mitigating information and evidence, under both state rules of professional conduct and *Brady v. Maryland* and its progeny.¹⁵³ In cases involving large amounts of ESI, defendants can argue that prosecutors can and should be held to a representation that none of the ESI possessed by their offices or by law enforcement contains exculpatory or mitigating information or evidence, or be required to produce it for meaningful review by defense counsel.¹⁵⁴
- 4. With the 2013 amendments to the Texas Code of Criminal Procedure, criminal defense counsel can argue that the legislature's intent is to mandate "open file" discovery by prosecutors' offices—discovery that should include ESI in native format. The 2013 amendments to the Code represent an effort by the legislature to "level the playing field" on pretrial access to information, among prosecutors and defense counsel. Criminal defense counsel can argue that access to native format ESI is essential to leveling the playing field, especially in cases in which the state has access to forensic experts who are analyzing the data. In a case in which the state will seek to prove its case through ESI, access to that ESI in native format can be analogized to access to DNA evidence needed for defense testing. For the reasons discussed above, permitting access to ESI in native format may be required—in the appropriate case—to achieve the objective of a level playing field expressed in the 2014 Code amendments.
- 5. A court may well decide in its discretion that requested e-discovery is not "material to any matter involved in the action," in the words of article 39.14. As an example, one court properly denied a defense request for the contents of a cell phone when the evidence showed that the cell phone was turned off at the time of the incident at issue in the case.¹⁵⁵

^{152.} Massimo v. State, 144 S.W.3d 210 (Tex. App.-Fort Worth 2004, no pet.) (e-mails).

^{153.} Tex. Disciplinary Rules Prof'l Conduct R. 3.08; Brady v. Maryland, 373 U.S. 83 (1963).

^{154.} Setting the Record Straight, p. 14.

^{155.} Branum v. State, 535 S.W.3d 217, 224-25 (Tex. App.-Fort Worth 2017, no pet.).

6. Finally, state prosecutors (just like their federal counterparts) should be mindful of the long-range effects of e-discovery on the cases they bring. The advent of electronic discovery platforms and records concerning access by defense counsel presents more fertile ground for claims of ineffective assistance of counsel.¹⁵⁶ The careful prosecutor will necessarily monitor the extent to which criminal defense counsel actually engages with the discovery process in general, inclucing through e-discovery as appropriate.

§ 25.9 ESI, Protective Orders, and Protection of Cooperating Witnesses and Claimed Victims

Another hot-button issue for prosecutors and government investigatory agencies with respect to production of ESI is the extent to which the production of ESI in a criminal case could potentially compromise or place in danger cooperating witnesses, victims, and ongoing investigations. This has always been an issue in certain types of criminal cases—even when discovery was all contained in paper records like hard-copy investigation and laboratory reports—but has heightened sensitivity for Texas state prosecutors with respect to records in electronic form.

The use of protective orders obviously militates against the risk that identities of cooperating witnesses and victims could be proliferated and disseminated. Many Texas prosecutor offices have standard agreements that defense counsel are required to sign as a condition of access to an electronic discovery platform. As previously discussed, a discovery protocol can be put in place that specifies that materials provided are not to be copied or disseminated by defense counsel. In addition, if ESI has been stored and organized properly, a Texas prosecutor's office and/or state law enforcement agency may well have the ability to conduct electronic searches within a particular data set for information that the state believes may put cooperating witnesses or claimed victims at potential jeopardy, such as personal identifying information (e.g., address, e-mail, phone information). The state can choose in the appropriate case to redact such personal identifying information from a production of e-discovery, subject of course to the ability of defense counsel to raise an issue about its non-production under the Texas Code of Criminal Procedure or otherwise. Some prosecutor offices around the state choose to do this type of redaction, and others (to avoid both the administrative burden and potential challenges) do not.

^{156.} See, e.g., Crawford v. State, No. 06-18-00140-CR, 2019 WL 1412239, at *4 (Tex. App.—Texarkana Mar. 29, 2019, pet. ref'd). For one discuss on of how the advent of e-discovery can impact ineffective assistance of counsel claims, see B. Garrett, *Big Data and Due Process*, 99 Cornell L. Rev. Online 207 (2014).

§ 25.10 Conclusion

As technology ever evolves, so does the impact on discovery in federal and state criminal cases. As the various considerations discussed in this chapter illustrate, the evolution and proliferation of electronic records has compelled prosecutors, defense counsel, and judges to become more conversant in the manner in which data relevant to criminal investigations and prosecutions is collected, stored, and made available in discovery. In any particular criminal case involving electronic records, there also exists the strong possibility that all data is not stored in a central repository, as it might be in a civil case involving a company that harvests data and places it in the control of an e-discovery vendor. Thus, the e-discovery challenges faced by prosecutors and defense counsel alike may well exceed those faced by their counterparts who litigate civil cases. These challenges can be faced effectively only if criminal law practitioners and courts are provided the tools and education to understand at least the basics—without becoming information technology professionals—of the manner, means, and mechanics of how electronic data can be created, harvested, stored, analyzed, and made available for discovery.

Chapter 26

Mobile Devices

Dan Regard¹

§ 26.1 Follow the Data

We are now in a golden age of data discovery. There is data everywhere!

With the massive adoption of mobile devices, it is natural that parties would seek to discover data from those sources. And because the devices may be constantly present, constantly powered on, and constantly connected, they can be a rich source of information.

However, as devices have become more evolved, the discovery of the data on those devices has become more complicated. Or at least it appears to be more complicated. This is a consequence of the rapid development cycle, device capabilities, architecture and technology advances, imbedded sensors, data privacy, Internet connectivity, and Software as a Service (SaaS) (software accessed online rather than installed on individual computers) as a deployment model.

This chapter presents a primer on mobile devices, but also serves as a methodology to approach discovery on any computer system. The focus, the theme, and the solution is to identify the device, but follow the data.

§ 26.1:1 Traditional Device Forensics

The traditional approach to mobile device forensics is to create a copy of the active, accessible portions of a device's storage. This is accomplished by copying the device using a variety of specialized equipment and software. Typically, the copy is stored in a single file (or a series of related files). That copy is often referred to as an "image."

A forensic image can fall into multiple versions: a bit-level copy (all accessible storage area with active, deleted, or zero data), a logical copy (all active file and data,

^{1.} Dan Regard is the Founder and CEO of Intelligent Discovery Solutions, Inc. He has worked with computers and litigation for over thirty years. Special thanks go to Hunter McMahon and Ken Marchese for their assistance in preparing this chapter.

which may include some deleted data within application storage areas), or a targeted copy (specific files or records). Of these, the logical copy is the most common.

Once the copy or image is made, forensic tools (software programs) are used to extract individual data streams, specific data files, run searches, and conduct other avenues of analysis. Bit-level copies can also be called bit-for-bit, bit-by-bit, bit-streaming, and other names. "Bit" is the flag to look for.

Sometimes the bit-level copy or logical copy can be restored to an empty device. This causes the new device to become a clone of the original device. This can be helpful for some types of inspections, especially when examining the original user's experience or testing how certain installed software works collectively. Clones can also be made to virtual machines. This allows the testing to be repeated while always reverting back to the original condition of the software and data at the time of collection.

Historically (in the past ten years) a common sequence of events was as follows: A party would request access to a device (typically a phone). The court would grant access. The device would be imaged. A copy would be provided to both parties, typically within bounds of a protective order. The image would be examined. The artifacts on the device may indicate files that were created, copied, or deleted, as well as when that activity took place, plus a strong inference as to who did it based on user accounts or access rights. An opinion, and possibly an opposing opinion, would be produced.

More recently, an inspection protocol might be put into place whereby an expert (either a neutral, or a restricted expert from the requesting party) can run a search on their copy of the image. Then the results are provided to the producing party for a responsiveness, privacy, or privilege review before the requesting party can access the search results.

There is nothing wrong with this approach. It works. It is easy to understand. It is easy to deal with (one device, one copy). It is compartmentalized (again, one device, one copy). It is finite. We still use it.

But as devices and Internet services have become more interconnected, the process has become more complicated. The device itself may only be part of the whole picture. Increased sensitivity to personal data, questions of ownership and access, and potential co-mingling of privileged material has made this more complicated. With that in mind, this chapter will provide a structure for dealing with the data that is commonly associated with mobile devices that will assist practitioners and judges in dealing with the leading edge of technology and data: discovery of mobile devices. Also, since mobile devices are really just computers on mobility steroids, the nomenclature and the techniques discussed here translate to almost any data discovery.

§ 26.1:2 Copying the Device (Imaging)

Making a copy of a mobile device, either a bit-level copy, a logical copy (active files only), or even a targeted (partial) copy is a capability that is in constant flux. This is because device manufacturers like Samsung and Apple are constantly improving passcode, data encryption, and other data security mechanisms. Additionally, developers like Facebook and Twitter are also changing encryption and setup at the application level. At the same time, developers of inspection software and equipment are constantly adjusting their own equipment and software to adapt to those changes by the manufacturers and application developers. It is a forensics game of cat and mouse.

This means that the capability to copy a device (or portions of a device), especially where the device owner may not be available or may not cooperate, may be impossible or severely limited. And those limitations may change over time. What was possible yesterday may not be possible today. What is not possible today, especially on the newest models and operating systems, may be possible tomorrow. Or it may never be possible.

For this reason there have been occasions when data extraction is not possible. For those circumstances, photographing the data as it is displayed on the device or even a manual documentation of a personal inspection can sometimes be the only solution, although this is rarely used. Another alternative is to collect specific data from alternative source locations.

§ 26.1:3 Alternative Source Locations

When considering mobile device data, it is also important to recognize that many data types (e.g., texts, e-mails, calendar entries, contacts, phone logs) may be available on other devices or in other source locations. This can be important when there are technical, encryption, or even geographic jurisdictional challenges. Below is a list of some of the alternative source locations where one might look for more accessible or more complete data sets, and some examples of each:

- Corporate servers—corporate e-mail
- Service providers—Google mail (Gmail) account, Twitter, Waze, wireless carriers

- Backups—iCloud, iTunes, older (idle) devices
- Synced devices—smartphones, tablets, laptops
- Destination devices—recipients of e-mails or texts
- Mobile device management (MDM)—corporate software that controls (and shadows) mobile usage

Each alternative source may have pros and cons. Each alternative source may retain data for different periods of time or slightly different sets of data. They may have more or different data than the targeted device.

For example, a wireless carrier may have records of SMS (Short Message Service) text or MMS (Multimedia Messaging Service) media messages sent via a text-messaging plan. But an iPhone combines these with iMessage. On the iPhone, MMS and SMS appear green and iMessages appear blue. The wireless carrier may have a longer history of SMS and MMS messages, but would have no equivalent record of the iMessages.

Similarly, it is possible to make calls using Zoom, Facebook, Skype and other applications. These calls would not appear in the wireless carrier phone records.

One of the historical characteristics of mobile devices (now changing) was the fairly limited storage space. This was a cause for limiting the data on the device. This is why data is often partially on a mobile device but more fully available on a corporate server or application server. The countervailing constraint was limited or sporadic bandwidth. This was a basis for keeping frequently used data on the device (a technique known as "caching").

For example, Apple iPhones allow users to specify keeping e-mail on the device for one day, three days, one week, two weeks, one month, or indefinitely. The choice the user makes will affect how many days of e-mail is on the device and, correspondingly, how much storage is used. Apple iPhones also allow users to keep specific text messages on the device for thirty days, one year, or forever.

Any one of these sources can provide alternative, and sometimes more cost effective and even richer data than a given mobile device. Due to specialty equipment and training, mobile device acquisition (copying) tends to cost more than normal computer copying or data extraction from targeted systems. Therefore alternatives should always be considered. When they are considered, the expanded options for mobile device data collection can be expanded as bit-level copy, logical copy, or targeted copy, plus photographs (or screenshots), personal inspection, or alternative sources.

The alternative sources have become even more important today because, as referenced earlier, data and devices are no longer synonymous. Devices can contain data that is uniquely on that device, but also contain data that is only partially on that device, allowing (or necessitating) the inclusion of alternative sources in order to gain a full picture of the targeted data. There is a model for considering all of the locations of the data. This is via the "four aspects of device data."

There are also extreme situations where data can sometimes be copied from secured or broken device by directly accessing the internal chips and pins. Such a "chip-off" is fascinating for us geeks, but beyond the scope of this chapter.

§ 26.1:4 The Four Aspects of Device Data

While a device may be a physical, singular object, the data associated with a given device does not have the same clear, well-defined boundaries. Rather, devices can be complete containers, partial containers, zero containers (data conduits), or triggers for external data systems. This is because today our systems are connected together. And mobile devices, especially smartphones and tablets and even laptops, are often used as local interfaces to remote cloud-based applications. This results in the data residing centrally. There may be a smaller subset stored locally to enhance the perception of speed (a cache). And the device itself may create data logs to track user activity for purposes of security, performance, troubleshooting, version control, and user preferences.

Understanding the four aspects is the key to conducting discovery on these devices. But before we talk about these categories of data, we need to also make sure we are focused on the data—that we *follow the data*. This is important because traditionally most people focus on the device (the container). Instead we should focus on the data (the content). This is the container versus content mind-shift.



Figure 26-1: Container view vs. content view

§ 26.1:5 Container vs. Content

As a result of device evolution, data that was entirely and uniquely located on a device and available once the device was secure is no longer guaranteed to be available on or from that a device. At the same time, devices are recording more types of data with more detail and for longer than ever before.

The impact is that a collection from a device may (a) not include everything you expect and (b) possibly include data that exceeds what you expected. Each of these aspects has distinct technical and legal challenges. Understanding these four aspects is critical to determining how to request, subpoena, or decide discovery issues related to such devices.

During the investigation of accounting restatement of a publicly traded company, one of the officers under investigation famously stated that investigators would never get the secretary's computer—"It's in the Atlantic." Today, as devices become more and more connected, and our mobile devices (phones, tablets, and laptops) become glorified modems, batteries, monitors, and keyboards rather than isolated computers, the ability to eradicate data by destroying a single device becomes harder and harder. If

you realized that your Facebook posts were something that you suddenly wanted to get rid of, physically destroying your smartphone would have little effect.

With the change in how devices are connected, the new way to think about data—and discovery—is to think about the content that is sought rather than that device most associated with that data.

For example, you may seek a custodian's e-mail, which you would assume is on the smartphone, but actually may not be. Instead the e-mail on the phone may be limited by time (only two weeks of that data is stored locally on the phone). You can view older e-mail on the phone only after a request is sent to the server. Older e-mail is then immediately downloaded on an as-needed basis. It is not otherwise "on" the device.

Further, some smartphones are configured to not download attachments or graphics unless specifically, individually requested. Copying what is "on the phone" will there-fore not include such items.

Besides being limited in time or content, the ability to copy e-mail that is on the phone may also be limited. For example, the popular iPhone e-mail has headers in the main data storage, but the body of the e-mail is in an encrypted "secure enclave," which cannot be accessed via most forensic tools (but there are always rumors . . .).

Further, when an iPhone is backed up to iCloud, not everything is stored in the backup, such as e-mail. If we restore the iPhone from backup, the e-mail needs to be restored separately by syncing to whichever e-mail accounts are setup on the iPhone. Other purchased content is recorded as to what a user purchased, but not the content itself. Installed songs, apps, or books from Apple are not stored in the backup. They are restored separately, and those restorations will be the latest version, not necessarily the version that was on previously on the phone.

As a result, while the e-mail is the target and the smartphone may be able to *access* all of the e-mail, it doesn't necessarily *store* all of the e-mail. Hence, it may not be the best location to collect the e-mail. And a motion to compel discovery of the smartphone (the device), if granted, may not produce the desired result (the data).

Instead, follow the data. By specifying the data sought ("We are seeking X, Y, and Z") rather than the container sought ("We want a copy of the iPhone for employee AAA"), discovery is more targeted. In my experience, after decades of working in electronic discovery, focusing on the data (not the device) will provide better clarity, better proportionality, and better solutions.

It may still result in parties agreeing that collecting the available data on a smartphone, albeit limited in scope, is faster and less expensive than other routes. It is better that this is an informed decision rather than an uninformed request.

§ 26.1:6 Examples of the Four Data Aspects

We have described devices having four aspects of data, each equally important, illustrated by the following:

Fully on the Device: This includes the operating system, log files, user data files, contacts (that have been synced), text messages, some application data, and e-mail headers.

Note: There may be data that is fully on the device (like e-mail bodies on iPhones) that is visible to the user on a one-at-a-time basis but cannot be captured with a bulk download.

Partially on the Device: This includes data that is limited on the device and is downloaded on an as-needed basis. This may represent older text messages, older e-mails, or other application data that is synced to a central storage server and is only partially available locally.

It is common to have data sets only available partially (caching). This is a technique used by computer systems to provide the perception of faster performance via local storage of the most recent data while using slower storage for the majority of the data. For example, websites may store the current and most likely choices locally, which leads to faster data loading, but also lag times when accessing unanticipated links. The cached values may be on the local device. The rest of the Internet is not.

Thru the Device (Data Conduit): This is data that is accessed via a device but is (typically) stored on a centralized server. This may typically be information accessed via an Internet browser, but many applications are also merely shells that rely on Internet connectivity and centralized storage for the data accessed.

Many applications on smartphones (Windows, Android, iOS) are engineered as local software applications that have an installed code base but access centrally stored data. Think of Google search, Netflix, Uber, or any number of other services where you must be connected to the Internet to use them.

Mobile Devices

Triggered by the Device: This is data that is captured by other systems and may never be stored on the device itself. This includes the corporate Wi-Fi log that tracks when a smartphone is registered to the Wi-Fi network, the cell phone carrier records that record when and where calls are made, the financial transactions that result from using near-field-communications (NFC) (e.g., ApplePay), or the Starbucks transactions that show that the device was used to pay for coffee (via a scanned barcode). These third-party systems can be very informative, and there may be clues on the device that they were engaged, but the body of the data is captured and stored elsewhere.

Table 26-1 provides a quick listing of other examples of data that may be fully, partially, via, or triggered by a device. These are typical findings, but actual findings may vary and conditions may change on any given day.

	Data type or source	Fully on the device	Partially on the device	Accessed via the device	Triggered by the device
1	Photos	Y			
2	Contacts	Y		. And Star	
3	Applications	Y			
4	Text Messages	Y			
5	WiFi Networks	Y			
6	Bluetooth Devices	Y			
7	E-mail		Y		
8	Browser History		Y		
9	Phone History		Y		Y
10	Facebook Content		Y	Y	
11	Twitter Content		Y	Y	
12	Website Content			Y	Y
13	Salesforce CRM			Y	
14	Bluetooth Connections			Y	Y
15	WiFi Connections	N. Banadra	and the	The same sta	Y
16	Cell Tower Locations				Y
17	GPS History	Y	Y	Y	Y

Table 26-1: Examples of data types and storage locations

Understanding these four aspects is the key to understanding how to request data, how to find data, and how to preserve data. Equally important is that the user with the device, or even the corporation issuing it, may not fully understand where data is created or stored. Like a Facebook status: "it's complicated."

It's also not unusual for a given inquiry to potentially impact many different types of data. Consider an inquiry to the Amazon Prime Video viewer history. Which movies have been viewed, purchased, or rented is stored at Amazon. Movies that are downloaded, to the extent they still are downloaded, would be reflected on the device and tracked at Amazon. When a local application was logged into and by which user may be stored locally. Where the device was during any specific activity may be stored locally, via the carrier or other navigation, or other external logs. This may also be reflected in financial records with Amazon, in the user's e-mail, or reflected in the debit card account at the user's bank. As a result, complete discovery may include the following:

- The device (locations, logins, users, app usage, recent downloads) (full and partial)
- The service provider (logins, user activity history, purchase and usage history) (thru)
- The phone carrier call detail records (CDRs) or location (triggered)
- E-mails (invoices from Amazon) (partial)
- Debit card records (triggered, with attenuation)

In traditional discovery (i.e., paper discovery) parties request specific documents or document categories, not entire filing cabinets. Mobile devices are comparable to filing cabinets. They contain a wide variety of data that may be colocated, but otherwise unrelated or even privileged.

Best practices, as documented by The Sedona Conference Database Principles, state that parties are entitled to only the data structures that contain relevant data; not the entire data container nor the entire data system, and perhaps not the entire individual record.²

^{2.} See The Sedona Conference, Database Principles: Addressing the Preservation & Production of Databases & Database Information in Civil Litigation, 15 Sedona Conf. J. 121 (2014) Principle 1, https://thesedonaconference.org/sites/default/files/publications/171-216%20Database%20 Principles_0.pdf.

Mobile Devices

The FBI, when executing data acquisition, often acquires entire devices, but then uses a "taint team" to limit (filter) the information from the device to conform with the limits of the subpoena, warrant, or writ. This is because device acquisition can be fast, but the data segregation can be time consuming, especially when investigating a data store under adversarial conditions. How this is frequently done in civil litigation is what the next section is about.

§ 26.1:7 Collect the Device, but Follow the Data

By now, you may be thinking that devices should not be collected wholesale. Not true. They often are, for very good reason. Copying specific data sets (e.g., just photos) or, even more challenging, partial data sets (e.g., just specific photos) can be time consuming, as is an examiner seeking all traces of activity related to a specific set of data. Furthermore, it may not be clear which files or records fit the need until the initial inspection has finished. Taking devices out of circulation is disruptive. Inspecting active devices can alter the very evidence you are looking for. Therefore, live inspections, in order to make targeted collections, can be time consuming and forensically dangerous.

Also, in the past few years we have seen the emergence of "remote kits," whereby forensic equipment is sent to a device user to conduct a self-copy with remote guidance. In the spring of 2020, this practice increased dramatically with the implementation of work-from-home ("WFH"), and social distancing. With these kits it is easier and more reliable to have the device user initiate a zero-variation process that copies the entire device rather than to work through the many scenarios possible in a targeted capture.

Then, if necessary, a reverse targeted capture can be done by the forensic technician working with the image while the custodian participates via a remote session where the data is already "preserved" and the original device is back in service.

As a result, even though, as a best practice, discovery should be focused on the data, preserving and collecting data is still often done by copying the entire device. This can be restated as "Copy the device, but follow the data."

§ 26.1:8 Preserve Timely

Not all data has identical retention schedules. User data, such as e-mails, texts, documents, and social media posts may seem to exist forever. And many systems are designed to do just that—keep data forever, or at least until they are changed intentionally.

However, contextual data—the logs that track user activity—often have retention schedules. This is because they are typically used for immediate trouble shooting or for data security monitoring. As such, they may capture an enormous volume of detailed system activity records, but only need that data for a very short amount of time.

Once the event is successfully completed, the log data may no longer have any business value and is purged due to the large volumes. This can mean retention schedules measured in months, weeks, minutes, or even milliseconds. Due to these schedules, these data sources will change unintentionally. Other activity logs only store the last event.For devices that remain in service, normal usage can change the records.

In one case, it was necessary to find out who had sent a particular e-mail from a particular e-mail account. Via subpoena, the e-mail account registration information was acquired, which provided an original IP addressed used when the account was set up. Via other subpoenas, it was possible to trace the IP address to a particular carrier and to a particular address. This tied the e-mail in question to one of the parties in litigation. This was the "smoking gun." However, if the requesting party had waited one more week, then the carrier records would have been lost due to their normal data retention schedule. Whew.

If the interest in investigating a mobile device is focused on such contextual data, then it is a best practice to preserve such data sooner rather than later. Otherwise it may expire in the normal course of device usage. This may mean preserving the device. It may also mean requesting logs created and maintained on "triggered" systems.

§ 26.1:9 Most Common Data Sought

People often ask, "What is a typical data request that involves mobile devices?" Having worked on hundreds of mobile device matters, we can list the data requests that are seen most often for smartphones:

- Test messaging (SMS/MMS/iMessage/etc.)
- Chat application messages (WhatsApp/Facebook Messenger/etc.)
- Web browser history

- Photographs/movies
- Location history
- Call and voice mail history

For specialty devices, such as Fitbits, Apple watches, and vehicles, the requested data typically is associated with the usage of that particular device and may need to be collected from their online portals.

§ 26.1:10 Possession, Custody, and Control

One of the legal aspects of device data is the question of possession, custody, and control.

It is not within the scope of this chapter to discuss the legal history, aspects, or requirements of possession, custody, and control. However, it is important to point out that mobile devices can interact with dozens of applications and websites in a given day. Within the full universe of systems and data generated, each of those applications or websites will have different user terms and conditions that may spell out, contractually, who has possession, custody, and control of some or all of the data associated with those systems.

By way of example, some online application service providers may host your data as "your data," but may also track who logs into your account, from where, and when as an internal security measure. Yet in some cases that access log may be more valuable than the data itself. It may not be clear who owns that security log.

These aspects of possession, custody, and control are further compounded by the fact that mobile devices are subject to other technical or legal aspects due to portability (to which jurisdictional laws apply), confusing ownership scenarios (thanks to bring-your-own-device policies) and evolving technical and privacy capabilities.

Each of these issues may be raised in the process of discovery by either side. Most of this can be handled by asking the following questions:

- 1. Who owns the device?
- 2. Who owns the data?
- 3. How can the data be acquired?

4. What is the proper legal mechanism to acquire the data (RFP, subpoena, letter rogatory, etc.)?

Given the potential uncertainty of possession, custody, and control, it is not uncommon to see parties send subpoenas to adversarial organizations as well as individual employees. You should not consider doing this as a first step, however, because organizations are more likely to consider the full range of legal duties, obligations, rights, and defenses, whereas individuals may not. This can lead to individuals changing, losing, deleting, or destroying data that might otherwise be preserved.

§ 26.1:11 Data Privacy

Mobile devices tend to be personal devices or, at minimum, have a lot of personal information on the devices. This ranges from family photographs to intimate messages to personal travel history at a very granular level. This can reflect on personal habits, health, sexual preferences, political persuasions, and religious practices.

In the U.S. this may trigger any number of a patchwork of federal, state, and local rules, such as the Health Insurance Portability and Privacy Act (HIPAA) and the California Consumer Privacy Act (CCPA). Globally, there are many data protection laws to deal with—most notably the European Union's General Data Protection Regulation (GDPR).

Mobile devices often mingle business data with personal data. Even people who carry two phones (or more) and feel that the explicit content is separated may find that the location history is identical and that location history can be very personal.

Similar to the comingling of personal and business communications, privileged materials may be comingled on mobile devices. At the same time, many times the data sought on mobile devices is contextual data reflecting activities, dates, times, and locations. Such contextual data is rarely privileged. Typically the fact of when, where, and how long someone met with counsel is not considered privileged. So is it with contextual data. Nonetheless, due to the potential for comingling, and the rich types, volumes, and granularity of data on modern systems, it is always a best practice to have a privilege clawback provision (e.g., Fed. R. Evid. 502) in place. This is more so for mobile devices.

For all of these reasons there is often a heightened sensitivity to collecting mobile devices. Some techniques for dealing with that sensitivity are the following:

- Put a protective order in place
- Put a clawback provision in place
- Put an inspection protocol in place
- Seek the data from a secondary, less comingled, device or location
- Engage a data neutral to collect and filter the data
- Allow the user to participate in the process

Depending on circumstances, some of these may be more practical than others. But having options is often the key to finding a viable path. Data privacy is a very important issue, domestically and internationally, but with proper preparation it can be dealt with.

§ 26.1:12 Remote Wiping and Inadvertent Changes

One particularly interesting aspect of mobile devices is that many of them are enabled with remote wiping. There is also after-market software (such as mobile device management) that can add this feature. This means that an authorized user can issue a remote command to erase all of the content. This could happen with an intent to deny discovery (e.g., a bad actor wants to wipe the device), could happen in the normal course of business (e.g., IT wipes the device of a former employee under standard security protocols). While this does not happen often, it remains a possibility to be considered, especially with respect to cevice preservation.

Similar to remote wiping, although not as black-and-white, is the fact that mobile devices may get updated inadvertently either by remaining online and receiving updates or by being turned on and syncing with various systems in a single burst.

In one case where a phone was secured in anticipation of an investigation, months later the device was turned on to confirm it was the correct device. That act of "checking the device" resulted in changes to the content, expiration of email beyond the twoweek setting, expiration of text messages beyond the one-month setting, downloads of revised posts, and a new data trail as to where the device was and when it was interacted with. Oops.

All of these scenarios can be addressed by disabling connectivity (putting the device in airplane mode) as soon as it is acquired, or by storing the device in a Faraday bag a mesh enclosure modeled off of the Faraday cage that prevents wireless signals, named for the 1836 inventor Michael Faraday. Once the data is secure and the device is returned, it can be switched back into service.

§ 26.1:13 Follow the Rules

Despite the fact that mobile devices can introduce new problems, exacerbate existing problems, and be generally intimidating, these can all be solved, and are being solved on a daily basis. The Federal Rules of Civil Procedure and their local equivalents work very well for all of these challenges. When clients have problems with mobile devices, turn to those rules:

- Is the discovery sought relevant?
- Is the discovery sought privileged?
- Is the discovery sought proportional?
- Is the discovery sought prejudicial?

By applying these well-established rules, we have successfully navigated a broad landscape of data sources and data devices. The rules work.

§ 26.1:14 Summary of Section 26.1

By now you have learned the following:

- Copy the device, but follow the data
- Act timely—some types of data expire on different schedules
- On a given device, certain data may be fully or partially or nominally available
- Some types of data are more commonly sought than others
- Consider alternative data locations
- Put protective orders, clawbacks, and inspection protocols in place
- Follow the rules

We find that the key to unraveling these challenges is to follow the data. Determining what is being sought, and for what purpose it will be used will allow all parties to better identify the data target and the proper technical and legal methods to discover it.

§ 26.2 Historical Background in Mobility

It used to be phones were just that: simple devices that allowed us to talk to one another. They had a single function, hung on a wall or sat on a table, and were permanently wired into our homes. During the 1990s cell phones removed the wires allowing us to roam around talking, but phones remained relatively simple devices for voice communications. That all changed in January 2007 when Apple introduced the iPhone. The iPhone wasn't the first smart mobile device; smart mobile devices had been around for decades. The Apple Newton, the Palm Pilot, and the Blackberry all preceded the iPhone, some by more than a decade. They were handheld mobile devices. They allowed for third-party applications. And the BlackBerry even had mobile data and e-mail capabilities. But the iPhone was the first device to merge increasingly high-speed mobile networks with the increasing speed and power available to mobile devices to provide a compelling user experience.

For years the limiting factor was how much storage the phone had. Was it 16 gigabytes, 32, 64, or more? The size of the phone's storage defined how much a user could do with it, how many photos they could take and movies they could record, how much music they could carry around with them, and how many apps they could run. But over time the networks the phones relied on increased in speed. Eventually (now with 5G) the networks got so fast that the data no longer needed to be stored on the phone itself, and the phone became an extension of other systems, a portal into a much larger universe of data and applications, and a hub for connecting and controlling other devices like home automation systems, smart watches, fitness trackers, and home security systems.

Today smartphones are the nexus for everything we do digitally. In many cases they know our health better than our doctors do. They know where we are and where we've been. They know where our office is and where home is, and generally what times we commute between the two. They know who we communicate with and how frequently. They know that we haven't called our mom in over a month and that we've ordered Chinese delivery eight times in the last four weeks. They remember almost everything about what we do, and in many cases, they remember it more accurately than we do ourselves.

Case in point: I met a friend at a conference in New York City last winter. We had been at the conference the year before and had eaten at a steakhouse in Manhattan. We had a great time and wanted to go back, but we couldn't remember the name or location of the restaurant. I pulled out my phone, checked my location history during the conference the prior year, and found nothing. The phone had no history of my having gone to a steakhouse in NYC during the prior year's conference. Confused, I searched the phone for all recent NYC trips, and what do you know, it found the restaurant. The phone knew that it had been a different trip to NYC when we had met and had dinner. It also knew exactly where the restaurant was, what time we arrived, and when we left. My phone knew more about where we had been and what we had done than the two of us could recall together.

Our mobile devices are windows into our lives, with our favorite one (the smartphone) sitting at the center, orchestrating the entire affair. Our smartphones and other mobile devices, contain and have access to incredibly detailed and comprehensive facts about who we are and what we do. And this data persists across device replacement. When we upgrade our devices, our data comes along with us, and our new device recalls all of the facts that our old one knew. Not only do our devices know these facts, they are better able to recall them than we are. The data provided by these devices can prove to be compelling evidence during litigation.

But what data is available, how do you get to it, how do you know what it means once you've got it, and what pitfalls await as you embark upon discovery of data originating from mobile devices?

Why the interest in mobile devices? Mobile devices have some characteristics that make them particularly attractive, or troublesome, depending on your perspective. They move around, so they can get lost, broken, and can become physically subject to different laws in different jurisdictions. They might be wearable (or fit in your pocket), so they can be very personal (and reflect personal activity). They have become an integrated part of how we communicate, how we learn, and how we remember, so they contain an almost unbroken sequence of events. They can have an overwhelming array of sensors, inputs, outputs, and connectivity protocols. This makes them rich in a wide variety of contextual data.

If you want to know who knew what and when, then there are few types of data that can provide those answers in as great of detail as the data captured on mobile devices.

§ 26.2:1 What Is a Mobile Device?

When discussing how mobile devices now and in the future can impact litigation, it's important to define exactly what a mobile device is. Is it a desktop computer? No. Is it a smartphone? Yes. Those are pretty easy to answer, but lying between those two points are a myriad of different devices that blur the lines between mobile and traditional computing environments.

§ 26.2:2 How to Determine If It's a Mobile Device

So how can we tell if a device is a mobile device or not? A few simple questions can narrow down the field. First, is it portable/can you carry it? Second, is it mobile? Can you pick it up and walk around with it with power and connectivity? Your desktop computer is *not* a mobile device. While it's portable (you can move it and then plug it in again), it's really not mobile. Third, is it always on? Does your device connect to the Internet (and other services) constantly?

Consider the smartphone. It has a battery, users generally charge the devices daily to keep them operating, and the device does not go into sleep mode or hibernate—it is always on and ready to be used. Similarly, for a wearable smart watch or Fitbit, the desired functionality of the device requires it to be constantly operational. This "always-on" property will prove to be a critical factor later when we discuss the depth of data available from mobile devices.

Device property	Desktop computer	Laptop computer	Tablet	iPad	Smart- phone	Smart watch
Is it portable?	No	Yes	Yes	Yes	Yes	Yes
Does it use a mobile OS?	No	No	Depends	Yes	Yes	Yes
Is it always on?	No	No	Depends	Yes	Yes	Yes
Does it have geolocation services?	No	No	Depends	Depends	Yes	Depends
Does it have wireless connectivity?	Depends	Yes	Yes	Yes	Yes	Yes
Is it tied to a hub device or cloud-based system?	No	No	Depends	Yes	Yes	Yes
Is it a mobile device?	No	No	Maybe	Yes	Yes	Yes

Table 26-2: Properties of mobile devices

Other aspects include geolocation services (GPS), wireless connectivity (cellular and Wi-Fi), and the degree to which the device stores applications and data locally or accesses them centrally.

In short, portability itself is not the defining characteristic of mobile devices. The defining characteristics of a mobile device is that it is a portable device with a specialized operating system and is "always-on."

When determining if a device is a mobile device or not, another factor to consider is that lines blur between mobile devices and IoT devices, making it very difficult to assess if a device is a mobile device or an IoT device. In fact, many mobile devices are also considered IoT devices as well, such as Fitbit.

The primary difference between a mobile device and a non-mobile IoT device is portability. Does a custodian pick it up and carry it around with them? Fitbit? Yes, mobile device. Nest Thermostat? No, non-mobile IoT device. Of course, as we will see later, non-mobile IoT devices commonly store data on mobile devices.

However, if you consider the four aspects of data, then it may not matter if a device is mobile. You may find that those four aspects allow you to understand any device and any data.

§ 26.2:3 Unexpected Mobile Devices

When considering mobile devices and thinking about what falls into the category and what doesn't, there are some devices that aren't obviously mobile devices but still fit the requirements. For example, how about an automobile? It's certainly mobile, it uses a specialized operating system, it has geolocation services and wireless connectivity, and in many cases it acts as a hub device and connects to other devices like wearables and smartphones.

The only caveat is that cars are not always-on. Or are they? We think of cars as being turned off when we turn them off and walk away, but is the car really turned off? The operating systems for certain modern cars continue to operate in reduced fashion when the car is turned off and can perform operations such as unlocking or remote starting. The emergence of software-integrated vehicles has created a question as to who owns the features, the software, and the data. These appear as computer devices, not mechanical devices.

§ 26.2:4 Mobile Device Technology

Before taking a deeper dive into mobile devices, the data they contain, and how it can impact litigation, we should first establish a foundational set of terms. The following are common terms that you will enccunter when discussing mobile devices (and in many cases any computer system), and you should be familiar with their proper definitions and usage.

App: Short for "application," an app is a software package that can be downloaded and installed on a mobile device. These are most commonly purchased from an authorized store that is provided by the developer of the mobile device's operating system. For example, on an iPhone this functionality is handled by the "App Store" and the Android device corollary is the "Google Play Store."

Backup: A backup of a device is a copy of the data and applications that are present on the device at a given point in time. A backup can be a complete copy of the device's storage (including the operating system and operating system data), all apps, and all local storage, or it can be limited to a backup for a single app or selected apps. Backups for devices such as iPhones and Android phones can occur without user interaction and be stored in the cloud services provided by the developer, iCloud and Google Drive, respectively.

Caching: Caching is the storage of small portions of frequently or recently used data locally to provide a better user experience when using other, slower data storage and retrieval equipment. Caching on the CPU can cause memory storage to appear faster. Storing in memory can cause disk drive storage to appear faster. Storing data locally can cause Internet connectivity and bandwidth to appear better and faster. Storing recent page views can cause Internet browsers to appear to work faster.

Caching is important in mobile forensics because it may result in data that is known to be remote, to also be stored locally, or for data that is perceived to be stored locally but truly stored remotely.

Cloud Computing: Infamously referred to as "simply someone else's computer," the cloud is an ecosystem comprised of systems that are accessed via the Internet. Common aspects of cloud computing are:

• Virtualization, meaning that one system is not tied directly to a single piece of hardware or equipment

- Multi-tenancy, meaning that multiple individuals or companies share content and resources from a single environment
- Remote access and management, meaning that access to the systems is provided via the Internet as opposed to residing on a company's local network, and that management of these systems is done remotely and not by physically accessing the device
- Rapid scalability, meaning that as demands for performance and capacity increase the systems can dynamically expand to meet those demands

One of the key factors about cloud computing that is applicable to litigation is that the cloud can retain data long after it has been removed from the mobile device. In general, mobile devices have limited storage capacity, which, while it can be quite large, can fill up quickly with video, photo, and other content. The devices will offload content to cloud services and are able to recall it quickly if the user requests it. In some situations, stub data (data that represents part of a record or part of an e-mail but not the entire record) can continue to reside on the mobile device, and in others there can be little or no indication that data is not present.

Database: A database is a collection of related data that is stored in a highly structured and specific format. For apps on mobile devices, databases are the most common format for data storage. For example, geolocation data would be stored in a database, as would chat message data. Databases are comprised of multiple related tables, which are roughly analogous to a tab in a spreadsheet where each column has a given name and is forced to match a specific format, for example, numeric, date/time, and text.

Encryption: Encryption is the conversion of data into a format that is unreadable by unauthorized individuals. A simple and ancient form of encryption is the Caesar Cypher, which is simply rotating the alphabet by a set number of letters. For example, a Caesar Cypher of 1 would turn the word "DOG" into "EPH." This is an easy form to crack and is unlikely to be used by itself in modern encryption, though it can be used as one step in modern encryption algorithms.

Other popular modern encryption algorithms include DES, TripleDES, AES, Blowfish, SHA, Rijndael, SSL, and TLS. When discussing encryption, there are three states of data that need to be considered: data at rest, data in use, and data in transit.

Data at rest on mobile devices is generally encrypted by the device's operating system as part of the overall storage encryption, and the individual apps generally do not
apply additional encryption, meaning that if the device itself can be unlocked, data residing on the device will be available.

Data in use is generally not encrypted today, but this is changing on a daily basis.

Data in transit is generally encrypted between the source and destination points using a protocol like SSL or TLS. This is the same as when you see the lock icon in an Internet browser indicating that the connection to the webserver is secure. Encryption in transit prevents eavesdroppers from listening in and reading the content of communications in transit.

With modern encryption it is very unlikely an investigator or analyst will be able to force their way past the encryption and access the data without the appropriate passwords and keys. Generally, these need to be provided by the device owner, but in some cases, such as when the device is owned and managed by an organization, the IT department may be able to open the encryption and access the device through an administrative process.

Forensics: Forensics is the process of scientifically investigating a device and extracting data and information related to the use of the device. Forensic analysis may be able to determine which applications were running on the device and when they were in operation. Forensics analysis may be able to recover deleted text messages or social media posts that are still resident on the device but that are flagged as deleted and don't appear to the end user, but the extent that this can be done is changing rapidly.

Wireless Connections (4G, LTE, 5G, Bluetooth, NFC, Wi-Fi, Mi-Fi, Li-Fi): These are how the device connects to other devices and to the Internet. One aspect of these connections is that the device will generally record which networks and devices it has connected to, when it was last connected, and potentially when it was first connected. A common example of this is using cell phone tower connection data to place a given phone to a given geographical location. Another example is to review the Wi-Fi connections that the device has connected to in order to determine if the device had ever been in a specific location (e.g., an office or coffee shop).

Much like the world of discovery requests, these terms can be used in a variety of ways, so you should make sure that when having conversations, propounding requests, and so forth, you are properly clarifying.

§ 26.2:5 Characteristics of Mobile Device Data

Three main characteristics of mobile data that are beneficial when viewed through the lens of litigation are objectivity, consistency, and persistence. This section describes what these mean and how they impact mobile device data discovery.

Objectivity: Objectivity means that the information recorded by the devices is not subject to an individual's perception of events but is instead collected by automated sensors and recorded by algorithm. As such, this is not subject to human bias or human error of precision.

For example, a person involved in a car accident might recall that it was really cold out and that they were driving the speed limit, and that there must have been ice on the road that caused their car to slide, resulting in an accident. All of that is subject to the person's individual experience and perception, their ability to recall events after the fact, and their desire to be factual in their recounting of events. All of these can be flawed, intentionally or unintentionally.

In contrast, sensors in the person's phone might tell the story differently. The sensors may have recorded that it was 45 degrees Fahrenheit and the vehicle was moving at 85 miles per hour. Or perhaps the data will corroborate the driver's version—it was 20 degrees out and the car was moving at 30 miles per hour. The inference is that ice was a distinct possibility and the vehicle's speed was not excessive for that portion of roadway. Either way, the data that resides on the phone will be objective in nature and not impacted by human bias or human recall.

Consistency: A second important aspect of mobile data is that it is consistent. This means that the data will be formatted and contain the same type of information for each data point recorded. This makes it much easier for data analysts to build models around the data and run analytics against it to determine standard behavior, deviation from standard behavior, and patterns.

But not only is it consistent in formatting, it's also consistent in recordation. Due to the always-on nature of mobile devices, the device itself will continue to collect data as long as it has power. There is no requirement for the user to do anything to initiate the collection of data, the device will collect the data on its own schedule.

For example, if geolocation information is being captured for a mobile device, we would expect that each time the device records the geolocation it will store the same information, likely (at a minimum) latitude, longitude, date, and time. This in turn

allows for the analysis of daily routines: where an individual goes each day (e.g., drop kids off at school, stop for coffee, go to work), where they eat lunch, when they leave the office, when they get home, and so on. Once a standard day is understood, one can analyze the data for anomalies. Are there days when the individual doesn't go to work? Are there days when they don't go home after work?

Case in point: my phone recently popped up a message telling me that it was going to take me twenty minutes longer to get to work due to traffic. Very helpful, but then I started wondering, when did I tell my phone where I work and when I leave for work? The answer is, I didn't. It figured it out on its own and was now using that information to provide me with useful information. The flip side to that is true as well—we can analyze data to determine where someone works, when they go there, and when they leave. In fact, we had one case where we were able to identify that an individual was moonlighting because we found two work locations he was consistently going to. In this case, it was helpful because he was suing one employer for work allegedly done off the clock, but at the same time was going to his second job while still on the clock for the first employer and with the first employer's equipment.

Persistence: Finally, persistence is a critical factor in mobile device data. Persistence means that the data continues to exist for very long periods of time and can persist beyond loss or destruction of the physical mobile device.

For example, a quick check of my Google geolocation data from my phone shows that it contains data going back almost five years. That predates my current phone, which means that the data is transferred from one phone to the next, again, being persistent. The data also persists in the Google Cloud, which means that if I lose my phone or if it breaks, the data continues to exist. We will discuss this in more depth later under the topic of the mobile device as a hub and endpoint data collector where data also resides in the cloud. For now, it's enough to know that the data is tenacious and persists over time and beyond the life of the mobile device.

§ 26.2:6 Understanding the Mobile Environment

Sometimes mobile devices are interconnected. In fact, this has become a business strategy for some companies. As a result, the mobile environment is a highly connected ecosystem consisting of multiple devices. One custodian might have a Fitbit, a smartwatch, a smartphone, and multiple other IoT devices (such as Nest Thermostats, Ring Home Alarm systems, Amazon Alexa, Google Home Devices, Phillips Hue Lights, and other connected devices) Due to battery and size constraints, many devices have only limited connectivity options, like Bluetooth. Bluetooth connections are limited by the physical distance between connected devices and require connections to be authorized. Generally this means that devices need to be nearby to communicate—within about thirty feet—and need to have previously gone through an authorization process before connections can be made.



Figure 26-2: Mobile device ecosystem

To compensate for this limited range, these devices will usually connect to a hub device. The hub device is most often a smartphone, although in some instances it can be a traditional computing system, such as a laptop or desktop computer. The hub device then collects information from the mobile device, retaining it locally, and relays the information up to a cloud provider.

§ 26.2:7 Mobile Devices in Litigation

When mobile devices are identified as a source for relevant electronic data, the primary issues are what data could one expect to be available on the mobile devices, and how that might impact the case. The types of data available on the device fall into two major categories: app data and operating system data. Each of these has two primary subsets: user data and forensic data.

User data is data that is readily apparent to the user and visible on the device without special tools. Forensic data, on the other hand, requires specialized tools and skills to collect, analyze, and report on. Forensic data includes deleted social media posts, detailed operating system logs, Wi-Fi network connection history, and app usage history for the device.

Types of Data Available: There are several types of data available from mobile devices. Sometimes the data is data intentionally created by the user, sometimes it is contextual data captured by the device to assist with trouble shooting or operations. Sometimes it is historical, previously erased data that can be recovered. Two major data types we see on mobile devices are below.

Data from Apps: Apps are what the custodian uses to interact with the device, for example, messaging, Facebook, LinkedIn, maps, and phone calls. App data is the content that is related to these apps and each app has its own data store. For example, Facebook posts reside in a database that is specific to Facebook.

User data is the data that everyone knows about, the social media post or "like," the ϵ mail message, the dates and times on calendar events, and so on. App data is exposed to the device user and is generally the reason for using the app in the first place.

Forensic analysis on these apps generally falls into two groups: recovering deleted items and revealing hidden data.

Recovering deleted items is exactly what it sounds like. When a user deletes a post cr message, that message is generally not immediately removed, it's simply flagged as "deleted" and continues to exist on the device for some amount of time. The longer the time—and the more the device is used—between the time of the deletion and the time the device is forensically collected, the higher the chance that data will be lost. But in many cases deleted items can be retrieved.

Revealing hidden data is slightly different. It's not deleted, it's simply additional data the app generates that is not exposed to the user.

Take text message read flags and dates, for example. Text messages don't always show which specific ones have been read or when they were read, but many apps track this type of information so they can show how many unread messages you have.

Data from the Operating System: The operating system is the behind-the-scenes master of the device and provides the apps with an environment in which to operate, providing security and access to the device's hardware. Operating system data includes things like known Wi-Fi networks, installed apps, file storage, and current date and time.

The user data managed by the operating system contains information including the user-defined username and device name, the applicable time zone, the installed applications, and the usage patterns of the user.

The forensic analysis of data captured and retained by the operating system includes the history of prior devices, prior applications, log files of the operation of the device, the battery power, the signal strength, the number of CPU cycles occupied by which applications every thirty seconds, and more. Much of this data is used by system engineers for troubleshooting and performance improvement. It can also be requests for relevant discovery purposes.

§ 26.2:8 Discovery Requests

As a final topic, I am often asked for examples of device and data requests. This is where the duality of devices and data come together. In early stages of litigation when trying to determine the data that likely exists, it is not uncommon to compile a list of the devices that were at play. The number, nature, and use of the devices will often inform the parties as to the types of data that may be available.

The following are examples of specific information sought through interrogatories (ROG) and requests for production (RFP) during a wage and hour dispute (e.g., overtime or missed meal/rest breaks).

- ROG: For each plaintiff, produce a list of dates on which you allege that the plaintiff was forced or permitted to work during disputed time.
- ROG: For each plaintiff, provide a list of all electronic devices such as smartphones, tablets, computers, wearables, etc., used by the plaintiff during any of the dates identified in Interrogatory X. Include in your response the make, model, operating system, date(s) of use, and description of the use.
- RFP: For each plaintiff, produce a metadata report for all text or chat messages (i.e., SMS, MMS, iMessage, WhatsApp, Facebook Messenger) sent or read during claimed work hours on any day identified in Interrogatory X and not already produced in Request Y. Metadata should include (at minimum): Source, Date and Time Sent, Date and Time Received, Read Status, From and To, Media/Attachment(s). Content is not requested at this time unless the message was to or from a defendant's employee.

- RFP: For each plaintiff, produce all GPS or other location data (e.g., from mobile devices, Google) during claimed work hours on any day identified in Interrogatory X. Data should include (at minimum): Date & Time, Location Data (i.e., latitude and longitude).
- RFP: For each plaintiff, produce a metadata report of all photos and video or audio recordings made during claimed work hours on any day identified in Interrogatory X. Metadata should include (at minimum): Source, Type of Media, Date & Time and Location Data. Content is not requested unless the location at which it was created is not available from the metadata and the photo, video, or audio recording tends to show the location.

It is important to note that each request is specifically designed to limit the information to only that which is needed (i.e., does not request the content unless to/from defendant's employee).

§ 26.2:9 Summary of Section 26.2

Having an understanding of what makes a device a mobile device should help you expand your definition of mobile devices and develop a broader appreciation of the multitude of computers that surround us (and record us) at all times. Distinguishing between user data and system data should help clarify how to ask for the data needed, but also minimize and navigate issues of proportionality and data privacy. Finally, examples of discovery requests should help all practitioners to focus on devices as sources, but data as the target. *Follow the data*.



Appendix A

Judicial Resources

General Resources

Ronald J. Hedges, Barbara J. Rothsteir, and Elizabeth C. Wiggins, *Managing Discovery of Electronic Information*, Federal Judicial Center Pocket Guide Series (3rd ed., 2017), www.fjc.gov/sites/default/files/materials/38/Managing%20Discovery%20 of%20Electronic%20Information_Third%20Edition_Second%20Printing_2019 .pdf

Timothy T. Lau and Emery G. Lee III, *Technology-Assisted Review for Discovery Requests: A Pocket Guide for Judges*, Federal Judicial Center (2017), www.fjc.gov/sites/default/files/2017/Technology-Assisted%20Review%20for%20Discovery%20Requests.pdf

Sean Broderick, et. al., *Criminal E-Discovery: A Pocket Guide for Judges*, Federal Judicial Center (2015), www.fjc.gov/sites/default/files/materials/06/Criminal%20 e-Discovery_First%20Edition_Third%20Printing_2019.pdf

Institute for the Advancement of the American Legal System, Unlocking E-Discovery: A Toolkit for Judges in State Courts Across the Nation (Oct. 2013), http:// iaals.du.edu/images/wygwam/documents/publications/Unlocking_E-Discovery_ Toolkit.pdf

Benchbook for U.S. District Court Judges, Federal Judicial Center (6th ed., Mar. 2013), www.fjc.gov/public/pdf.nsf/lookup/Benchbook-US-District-Judges-6TH-FJC-MAR-2013-Public.pdf/\$file/Benchbook-US-District-Judges-6TH-FJC -MAR-2013-Public.pdf

Maura R. Grossman and Gordon V. Cormack, *The Grossman-Cormack Glossary of Technology-Assisted Review*, 2013 Fed. Cts. L. Rev. 7(1) (2013), www.fclr.org/fclr/articles/html/2010/grossman.pdf

Institute for the Advancement of the American Legal System, *Navigating the Hazards* of E-Discovery, A Manual for Judges in State Courts Across the Nation (2d ed., 2012), http://iaals.du.edu/images/wygwam/documents/publications/Navigating_ eDiscovery_2nd_Edition.pdf

Appendix A

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery* of Electronically-Stored Information (Aug. 2006), http://ncsc.contentdm.oclc.org/ cdm/singleitem/collection/civil/id/56/rec/18

David K. Isom, *Electronic Discovery Primer for Judges*, Fed. Cts. L. Rev. 1 (2005), www.fclr.org/fclr/articles/html/2005/fedctslrev1.pdf

Guidelines for Cases Involving Electronically Stored Information, United States District Court for the Northern District of California, **www.cand.uscourts.gov** /filelibrary/1117/ESI_Guidelines-12-1-2015.pdf.

Principles for the Discovery of Electronically Stored Information in Civil Cases, District of Maryland, **www.mdd.uscourts.gov/sites/mdd/files/ESI-Principles.pdf**

Guidelines for Cases Involving Electronically Stored Information (United States District Court for the District of Kansas 2013), http://ksd.uscourts.gov/wp-content/ uploads/2015/10/Guidelines-for-cases-involving-ESI-July-18-2013.pdf

See also compilation of local rules, forms and guidelines done by K&L Gates: www.ediscoverylaw.com/local-rules-forms-and-guidelines-of-united-states -district-courts-addressing-e-discovery-issues/

In addition, the Sedona Conference has many publications addressing, in part, legal holds, defensible disposition, social media, BYOD, practice pointers for responding to discovery requests, proportionality, TAR, "Possession, Custody, or Control," privacy and ethics. These publications can be found at: https://thesedonaconference.org/publications.

Appendix B

Select Federal Rules of Civil Procedure

(As of December 1, 2019)

Rule 1—Scope and Purpose

These rules govern the procedure in all civil actions and proceedings in the United States district courts, except as stated in Rule 81. They should be construed, administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every action and proceeding.

2015 Advisory Committee Notes

Rule 1 is amended to emphasize that just as the court should construe and administer these rules to secure the just, speedy, and inexpensive determination of every action, so the parties share the responsibility to employ the rules in the same way. Most lawyers and parties cooperate to achieve these ends. But discussions of ways to improve the administration of civil justice regularly include pleas to discourage over-use, misuse, and abuse of procedural tools that increase cost and result in delay. Effective advocacy is consistent with—and inceed depends upon—cooperative and proportional use of procedure.

This amendment does not create a new or independent source of sanctions. Neither does it abridge the scope of any other cf these rules.

Rule 16—Pretrial Conferences; Scheduling; Management

- (a) *Purposes of a Pretrial Conference*. In any action, the court may order the attorneys and any unrepresented parties to appear for one or more pretrial conferences for such purposes as:
 - (1) expediting disposition of the action;
 - (2) establishing early and continuing control so that the case will not be protracted because of lack of management;
 - (3) discouraging wasteful pretrial activities;

- (4) improving the quality of the trial through more thorough preparation; and
- (5) facilitating settlement.
- (b) Scheduling.
 - Scheduling Order. Except in categories of actions exempted by local rule, the district judge—or a magistrate judge when authorized by local rule—must issue a scheduling order:
 - (A) after receiving the parties' report under Rule 26(f); or
 - (B) after consulting with the parties' attorneys and any unrepresented parties at a scheduling conference.
 - (2) Time to Issue. The judge must issue the scheduling order as soon as practicable, but unless the judge finds good cause for delay, the judge must issue it within the earlier of 90 days after any defendant has been served with the complaint or 60 days after any defendant has appeared.
 - (3) Contents of the Order.
 - (A) Required Contents. The scheduling order must limit the time to join other parties, amend the pleadings, complete discovery, and file motions.
 - (B) Permitted Contents. The scheduling order may:
 - (i) modify the timing of disclosures under Rules 26(a) and 26(e)(1);
 - (ii) modify the extent of discovery;
 - (iii) provide for disclosure, discovery, or preservation of electronically stored information;
 - (iv) include any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after information is produced, including agreements reached under Federal Rule of Evidence 502;
 - (v) direct that before moving for an order relating to discovery, the movant must request a conference with the court;
 - (vi) set dates for pretrial conferences and for trial; and

(vii) include other appropriate matters.

- (4) Modifying a Schedule. A schedule may be modified only for good cause and with the judge's consent.
- (c) Attendance and Matters for Consideration at a Pretrial Conference.
 - (1) Attendance. A represented party must authorize at least one of its attorneys to make stipulations and admissions about all matters that can reasonably be anticipated for discussion at a pretrial conference. If appropriate, the court may require that a party or its representative be present or reasonably available by other means to consider possible settlement.
 - (2) Matters for Consideration. At any pretrial conference, the court may consider and take appropriate action on the following matters:
 - (A) formulating and simplifying the issues, and eliminating frivolous claims or defenses;
 - (B) amending the pleadings if necessary or desirable;
 - (C) obtaining admissions and stipulations about facts and documents to avoid unnecessary proof, and ruling in advance on the admissibility of evidence;
 - (D) avoiding unnecessary proof and cumulative evidence, and limiting the use of testimony under Federal Rule of Evidence 702;
 - (E) determining the appropriateness and timing of summary adjudication under Rule 56;
 - (F) controlling and scheduling discovery, including orders affecting disclosures and discovery under Rule 26 and Rules 29 through 37;
 - (G) identifying witnesses and documents, scheduling the filing and exchange of any pretrial briefs, and setting dates for further conferences and for trial;
 - (H) referring matters to a magistrate judge or a master;
 - (I) settling the case and using special procedures to assist in resolving the dispute when authorized by statute or local rule;
 - (J) determining the form and content of the pretrial order;

- (K) disposing of pending motions;
- (L) adopting special procedures for managing potentially difficult or protracted actions that may involve complex issues, multiple parties, difficult legal questions, or unusual proof problems;
- (M) ordering a separate trial under Rule 42(b) of a claim, counterclaim, crossclaim, third-party claim, or particular issue;
- (N) ordering the presentation of evidence early in the trial on a manageable issue that might, on the evidence, be the basis for a judgment as a matter of law under Rule 50(a) or a judgment on partial findings under Rule 52(c);
- (O) establishing a reasonable limit on the time allowed to present evidence; and
- (P) facilitating in other ways the just, speedy, and inexpensive disposition of the action.
- (d) *Pretrial Orders*. After any conference under this rule, the court should issue an order reciting the action taken. This order controls the course of the action unless the court modifies it.
- (e) *Final Pretrial Conference and Orders.* The court may hold a final pretrial conference to formulate a trial plan, including a plan to facilitate the admission of evidence. The conference must be held as close to the start of trial as is reasonable, and must be attended by at least one attorney who will conduct the trial for each party and by any unrepresented party. The court may modify the order issued after a final pretrial conference only to prevent manifest injustice.
- (f) Sanctions.
 - In General. On motion or on its own, the court may issue any just orders, including those authorized by Rule 37(b)(2)(A)(ii)-(vii), if a party or its attorney:
 - (A) fails to appear at a scheduling or other pretrial conference;
 - (B) is substantially unprepared to participate—or does not participate in good faith—in the conference; or
 - (C) fails to obey a scheduling or other pretrial order.
 - (2) Imposing Fees and Costs. Instead of or in addition to any other sanction, the court must order the party, its attorney, or both to

pay the reasonable expenses—including attorney's fees incurred because of any noncompliance with this rule, unless the noncompliance was substantially justified or other circumstances make an award of expenses unjust.

2006 Advisory Committee Notes

The amendment to Rule 16(b) is designed to alert the court to the possible need to address the handling of discovery of electronically stored information early in the litigation if such discovery is expected to occur. Rule 26(f) is amended to direct the parties to discuss discovery of electronically stored information if such discovery is contemplated in the action. Form 35 is amended to call for a report to the court about the results of this discussion. In many instances, the court's involvement early in the litigation will help avoid difficulties that might otherwise arise.

Rule 16(b) is also amended to include among the topics that may be addressed in the scheduling order any agreements that the parties reach to facilitate discovery by minimizing the risk of waiver of privilege or work-product protection. Rule 26(f) is amended to add to the discovery plan the parties' proposal for the court to enter a case-management or other order adopting such an agreement. The parties may agree to various arrangements. For example, they may agree to initial provision of requested materials without waiver of privilege or protection to enable the party seeking production to designate the materials desired or protection for actual production, with the privilege review of only those materials to follow. Alternatively, they may agree that if privileged or protected information is inadvertently produced, the producing party may by timely notice assert the privilege or protection and obtain return of the materials without waiver. Other arrangements are possible. In most circumstances, a party who receives information under such an arrangement cannot assert that production of the information waived a claim of privilege or of protection as trial-preparation material.

An order that includes the parties' agreement may be helpful in avoiding delay and excessive cost in discovery. See Manual for Complex Litigation (4th) §11.446. Rule 16(b)(6) recognizes the propriety of including such agreements in the court's order. The rule does not provide the court with authority to enter such a case-management or other order without party agreement, or limit the court's authority to act on motion.

Changes Made After Publication and Comment. This recommendation is of a modified version of the proposal as published. Subdivision (b)(6) was modified to eliminate the references to "adopting" agreements for "protection against waiving"

Appendix B

privilege. It was feared that these words might seem to promise greater protection than can be assured. In keeping with changes to Rule 26(b)(5)(B), subdivision (b)(6) was expanded to include agreements for asserting claims of protection as trial-preparation materials. The Committee Note was revised to reflect the changes in the rule text.

2015 Advisory Committee Notes

The provision for consulting at a scheduling conference by "telephone, mail, or other means" is deleted. A scheduling conference is more effective if the court and parties engage in direct simultaneous communication. The conference may be held in person, by telephone, or by more sophisticated electronic means.

The time to issue the scheduling order is reduced to the earlier of 90 days (not 120 days) after any defendant has been served, or 60 days (not 90 days) after any defendant has appeared. This change, together with the shortened time for making service under Rule 4(m), will reduce delay at the beginning of litigation. At the same time, a new provision recognizes that the court may find good cause to extend the time to issue the scheduling order. In some cases it may be that the parties cannot prepare adequately for a meaningful Rule 26(f) conference and then a scheduling conference in the time allowed. Litigation involving complex issues, multiple parties, and large organizations, public or private, may be more likely to need extra time to establish meaningful collaboration between counsel and the people who can supply the information needed to participate in a useful way. Because the time for the Rule 26(f) conference or order, an order extending the time for the scheduling conference will also extend the time for the Rule 26(f) conference will also extend the time for the Rule 26(f) conference. But in most cases it will be desirable to hold at least a first scheduling conference in the time set by the rule.

Three items are added to the list of permitted contents in Rule 16(b)(3)(B).

The order may provide for preservation of electronically stored information, a topic also added to the provisions of a discovery plan under Rule 26(f)(3)(C). Parallel amendments of Rule 37(e) recognize that a duty to preserve discoverable information may arise before an action is filed.

The order also may include agreements incorporated in a court order under Evidence Rule 502 controlling the effects of disclosure of information covered by attorney-client privilege or work-product protection, a topic also added to the provisions of a discovery plan under Rule 26(f)(3)(D).

Finally, the order may direct that before filing a motion for an order relating to discovery the movant must request a conference with the court. Many judges who hold such conferences find them an efficient way to resolve most discovery disputes without the delay and burdens attending a formal motion, but the decision whether to require such conferences is left to the discretion of the judge in each case.

Rule 26—Duty to Disclose; General Provisions Governing Discovery

- (a) Required Disclosures.
 - (1) Initial Disclosure.
 - (A) In General. Except as exempted by Rule 26(a)(1)(B) or as otherwise stipulated or ordered by the court, a party must, without awaiting a discovery request, provide to the other parties:
 - (i) the name and, if known, the address and telephone number of each individual likely to have discoverable information—along with the subjects of that information that the disclosing party may use to support its claims or defenses, unless the use would be solely for impeachment;
 - (ii) a copy—or a description by category and location—of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment;
 - (iii) a computation of each category of damages claimed by the disclosing party—who must also make available for inspection and copying as under Rule 34 the documents or other evidentiary material, unless privileged or protected from disclosure, on which each computation is based, including materials bearing on the nature and extent of injuries suffered; and
 - (iv) for inspection and copying as under Rule 34, any insurance agreement under which an insurance business may be liable to satisfy all or part of a possible judgment in the action or to indemnify or reimburse for payments made to satisfy the judgment.
 - (B) Proceedings Exempt from Initial Disclosure. The following pro-

ceedings are exempt from initial disclosure:

- (i) an action for review on an administrative record;
- (ii) a forfeiture action in rem arising from a federal statute;
- (iii) a petition for habeas corpus or any other proceeding to challenge a criminal conviction or sentence;
- (iv) an action brought without an attorney by a person in the custody of the United States, a state, or a state subdivision;
- (v) an action to enforce or quash an administrative summons or subpoena;
- (vi) an action by the United States to recover benefit payments;
- (vii) an action by the United States to collect on a student loan guaranteed by the United States;
- (viii) a proceeding ancillary to a proceeding in another court; and
- (ix) an action to enforce an arbitration award.
- (C) Time for Initial Disclosures—In General. A party must make the initial disclosures at or within 14 days after the parties' Rule 26(f) conference unless a different time is set by stipulation or court order, or unless a party objects during the conference that initial disclosures are not appropriate in this action and states the objection in the proposed discovery plan. In ruling on the objection, the court must determine what disclosures, if any, are to be made and must set the time for disclosure.
- (D) Time for Initial Disclosures—For Parties Served or Joined Later. A party that is first served or otherwise joined after the Rule 26(f) conference must make the initial disclosures within 30 days after being served or joined, unless a different time is set by stipulation or court order.
- (E) Basis for Initial Disclosure; Unacceptable Excuses. A party must make its initial disclosures based on the information then reasonably available to it. A party is not excused from making its disclosures because it has not fully investigated the case or because it challenges the sufficiency of another party's disclosures or because another party has not made its disclosures.
- (2) Disclosure of Expert Testimony.

- (A) In General. In addition to the disclosures required by Rule 26(a)(1), a party must disclose to the other parties the identity of any witness it may use at trial to present evidence under Federal Rule of Evidence 702, 703, or 705.
- (B) Witnesses Who Must Provide a Written Report. Unless otherwise stipulated or ordered by the court, this disclosure must be accompanied by a written report—prepared and signed by the witness—if the witness is one retained or specially employed to provide expert testimony in the case or one whose duties as the party's employee regularly involve giving expert testimony. The report must contain:
 - (i) a complete statement of all opinions the witness will express and the basis and reasons for them;
 - (ii) the facts or data considered by the witness in forming them;
 - (iii) any exhibits that will be used to summarize or support them;
 - (iv) the witness's qualifications, including a list of all publications authored in the previous 10 years;
 - (v) a list of all other cases in which, during the previous 4 years, the witness testified as an expert at trial or by deposition; and
 - (vi) a statement of the compensation to be paid for the study and testimony in the case.
- (C) Witnesses Who Do Not Provide a Written Report. Unless otherwise stipulated or ordered by the court, if the witness is not required to provide a written report, this disclosure must state:
 - the subject matter on which the witness is expected to present evidence under Federal Rule of Evidence 702, 703, or 705; and
 - (ii) a summary of the facts and opinions to which the witness is expected to testify.
- (D) Time to Disclose Expert Testimony. A party must make these disclosures at the times and in the sequence that the court orders. Absent a stipulation or a court order, the disclosures must be

made:

- (i) at least 90 days before the date set for trial or for the case to be ready for trial; or
- (ii) if the evidence is intended solely to contradict or rebut evidence on the same subject matter identified by another party under Rule 26(a)(2)(B) or (C), within 30 days after the other party's disclosure.
- (E) Supplementing the Disclosure. The parties must supplement these disclosures when required under Rule 26(e).
- (3) Pretrial Disclosures.
 - (A) In General. In addition to the disclosures required by Rule 26(a)(1) and (2), a party must provide to the other parties and promptly file the following information about the evidence that it may present at trial other than solely for impeachment:
 - the name and, if not previously provided, the address and telephone number of each witness—separately identifying those the party expects to present and those it may call if the need arises;
 - (ii) the designation of those witnesses whose testimony the party expects to present by deposition and, if not taken stenographically, a transcript of the pertinent parts of the deposition; and
 - (iii) an identification of each document or other exhibit, including summaries of other evidence—separately identifying those items the party expects to offer and those it may offer if the need arises.
 - (B) Time for Pretrial Disclosures; Objections. Unless the court orders otherwise, these disclosures must be made at least 30 days before trial. Within 14 days after they are made, unless the court sets a different time, a party may serve and promptly file a list of the following objections: any objections to the use under Rule 32(a) of a deposition designated by another party under Rule 26(a)(3)(A)(ii); and any objection, together with the grounds for it, that may be made to the admissibility of materials identified under Rule 26(a)(3)(A)(iii). An objection not so made—except

for one under Federal Rule of Evidence 402 or 403—is waived unless excused by the court for good cause.

- (4) Form of Disclosures. Unless the court orders otherwise, all disclosures under Rule 26(a) must be in writing, signed, and served.
- (b) Discovery Scope and Limits.
 - (1) Scope in General. Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.
 - (2) Limitations on Frequency and Extent.
 - (A) When Permitted. By order, the court may alter the limits in these rules on the number of depositions and interrogatories or on the length of depositions under Rule 30. By order or local rule, the court may also limit the number of requests under Rule 36.
 - (B) Specific Limitations on Electronically Stored Information. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.
 - (C) When Required. On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:
 - (i) the discovery sought is unreasonably cumulative or

duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;

- (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
- (iii) the proposed discovery is outside the scope permitted by Rule 26(b)(1).
- (3) Trial Preparation: Materials.
 - (A) Documents and Tangible Things. Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent). But, subject to Rule 26(b)(4), those materials may be discovered if:
 - (i) they are otherwise discoverable under Rule 26(b)(1); and
 - (ii) the party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means.
 - (B) Protection Against Disclosure. If the court orders discovery of those materials, it must protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation.
 - (C) Previous Statement. Any party or other person may, on request and without the required showing, obtain the person's own previous statement about the action or its subject matter. If the request is refused, the person may move for a court order, and Rule 37(a)(5) applies to the award of expenses. A previous statement is either:
 - (i) a written statement that the person has signed or otherwise adopted or approved; or
 - (ii) a contemporaneous stenographic, mechanical, electrical, or other recording—or a transcription of it—that recites substantially verbatim the person's oral statement.
- (4) Trial Preparation: Experts.
 - (A) Deposition of an Expert Who May Testify. A party may depose

any person who has been identified as an expert whose opinions may be presented at trial. If Rule 26(a)(2)(B) requires a report from the expert, the deposition may be conducted only after the report is provided.

- (B) Trial-Preparation Protection for Draft Reports or Disclosures. Rules 26(b)(3)(A) and (B) protect drafts of any report or disclosure required under Rule 26(a)(2), regardless of the form in which the draft is recorded.
- (C) Trial-Preparation Protection for Communications Between a Party's Attorney and Expert Witnesses. Rules 26(b)(3)(A) and (B) protect communications between the party's attorney and any witness required to provide a report under Rule 26(a)(2)(B), regardless of the form of the communications, except to the extent that the communications:
 - (i) relate to compensation for the expert's study or testimony;
 - (ii) identify facts or data that the party's attorney provided and that the expert considered in forming the opinions to be expressed; or
 - (iii) identify assumptions that the party's attorney provided and that the expert relied on in forming the opinions to be expressed.
- (D) Expert Employed Only for Trial Preparation. Ordinarily, a party may not, by interrogatories or deposition, discover facts known or opinions held by an expert who has been retained or specially employed by another party in anticipation of litigation or to prepare for trial and who is not expected to be called as a witness at trial. But a party may do so only:
 - (i) as provided in Rule 35(b); or
 - (ii) on showing exceptional circumstances under which it is impracticable for the party to obtain facts or opinions on the same subject by other means.
- (E) Payment. Unless manifest injustice would result, the court must require that the party seeking discovery:
 - (i) pay the expert a reasonable fee for time spent in responding to discovery under Rule 26(b)(4)(A) or (D); and

- (ii) for discovery under (D), also pay the other party a fair portion of the fees and expenses it reasonably incurred in obtaining the expert's facts and opinions.
- (5) Claiming Privilege or Protecting Trial-Preparation Materials.
 - (A) Information Withheld. When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial-preparation material, the party must:
 - (i) expressly make the claim; and
 - (ii) describe the nature of the documents, communications, or tangible things not produced or disclosed—and do so in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the claim.
 - (B) Information Produced. If information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.
- (c) Protective Orders.
 - (1) In General. A party or any person from whom discovery is sought may move for a protective order in the court where the action is pending—or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken. The motion must include a certification that the movant has in good faith conferred or attempted to confer with other affected parties in an effort to resolve the dispute without court action. The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or

undue burden or expense, including one or more of the following:

- (A) forbidding the disclosure or discovery;
- (B) specifying terms, including time and place or the allocation of expenses, for the disclosure or discovery;
- (C) prescribing a discovery method other than the one selected by the party seeking discovery;
- (D) forbidding inquiry into certain matters, or limiting the scope of disclosure or discovery to certain matters;
- (E) designating the persons who may be present while the discovery is conducted;
- (F) requiring that a deposition be sealed and opened only on court order;
- (G) requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way; and
- (H) requiring that the parties simultaneously file specified documents or information in sealed envelopes, to be opened as the court directs.
- (2) Ordering Discovery. If a motion for a protective order is wholly or partly denied, the court may, on just terms, order that any party or person provide or permit discovery.
- (3) Awarding Expenses. Rule 37(a)(5) applies to the award of expenses.
- (d) Timing and Sequence of Discovery.
 - (1) Timing. A party may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except in a proceeding exempted from initial disclosure under Rule 26(a)(1)(B), or when authorized by these rules, by stipulation, or by court order.
 - (2) Early Rule 34 Requests.
 - (A) Time to Deliver. More than 21 days after the summons and complaint are served on a party, a request under Rule 34 may be

delivered:

- (i) to that party by any other party, and
- (ii) by that party to any plaintiff or to any other party that has been served.
- (B) When Considered Served. The request is considered to have been served at the first Rule 26(f) conference.
- (3) Sequence. Unless the parties stipulate or the court orders otherwise for the parties' and witnesses' convenience and in the interests of justice:
 - (A) methods of discovery may be used in any sequence; and
 - (B) discovery by one party does not require any other party to delay its discovery.
- (e) Supplementing Disclosures and Responses.
 - In General. A party who has made a disclosure under Rule 26(a)—or who has responded to an interrogatory, request for production, or request for admission—must supplement or correct its disclosure or response:
 - (A) in a timely manner if the party learns that in some material respect the disclosure or response is incomplete or incorrect, and if the additional or corrective information has not otherwise been made known to the other parties during the discovery process or in writing; or
 - (B) as ordered by the court.
 - (2) Expert Witness. For an expert whose report must be disclosed under Rule 26(a)(2)(B), the party's duty to supplement extends both to information included in the report and to information given during the expert's deposition. Any additions or changes to this information must be disclosed by the time the party's pretrial disclosures under Rule 26(a)(3) are due.
- (f) Conference of the Parties; Planning for Discovery.
 - Conference Timing. Except in a proceeding exempted from initial disclosure under Rule 26(a)(1)(B) or when the court orders otherwise, the parties must confer as soon as practicable—and in

any event at least 21 days before a scheduling conference is to be held or a scheduling order is due under Rule 16(b).

- (2) Conference Content; Parties' Responsibilities. In conferring, the parties must consider the nature and basis of their claims and defenses and the possibilities for promptly settling or resolving the case; make or arrange for the disclosures required by Rule 26(a)(1); discuss any issues about preserving discoverable information; and develop a proposed discovery plan. The attorneys of record and all unrepresented parties that have appeared in the case are jointly responsible for arranging the conference, for attempting in good faith to agree on the proposed discovery plan, and for submitting to the court within 14 days after the conference a written report outlining the plan. The court may order the parties or attorneys to attend the conference in person.
- (3) Discovery Plan. A discovery plan must state the parties' views and proposals on:
 - (A) what changes should be made in the timing, form, or requirement for disclosures under Rule 26(a), including a statement of when initial disclosures were made or will be made;
 - (B) the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused on particular issues:
 - (C) any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced;
 - (D) any issues about claims of privilege or of protection as trialpreparation materials, including—if the parties agree on a procedure to assert these claims after production—whether to ask the court to include their agreement in an order under Federal Rule of Evidence 502;
 - (E) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed; and
 - (F) any other orders that the court should issue under Rule 26(c) or under Rule 16(b) and (c).

Appendix B

- (4) Expedited Schedule. If necessary to comply with its expedited schedule for Rule 16(b) conferences, a court may by local rule:
 - (A) require the parties' conference to occur less than 21 days before the scheduling conference is held or a scheduling order is due under Rule 16(b); and
 - (B) require the written report outlining the discovery plan to be filed less than 14 days after the parties' conference, or excuse the parties from submitting a written report and permit them to report orally on their discovery plan at the Rule 16(b) conference.
- (g) Signing Disclosures and Discovery Requests, Responses, and Objections.
 - (1) Signature Required; Effect of Signature. Every disclosure under Rule 26(a)(1) or (a)(3) and every discovery request, response, or objection must be signed by at least one attorney of record in the attorney's own name—or by the party personally, if unrepresented—and must state the signer's address, e-mail address, and telephone number. By signing, an attorney or party certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry:
 - (A) with respect to a disclosure, it is complete and correct as of the time it is made; and
 - (B) with respect to a discovery request, response, or objection, it is:
 - (i) consistent with these rules and warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law, or for establishing new law;
 - (ii) not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and
 - (iii) neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action.
 - (2) Failure to Sign. Other parties have no duty to act on an unsigned disclosure, request, response, or objection until it is signed, and the court must strike it unless a signature is promptly supplied after the omission is called to the attorney's or party's attention.

(3) Sanction for Improper Certification. If a certification violates this rule without substantial justification, the court, on motion or on its own, must impose an appropriate sanction on the signer, the party on whose behalf the signer was acting, or both. The sanction may include an order to pay the reasonable expenses, including attorney's fees, caused by the violation.

2006 Advisory Committee Notes

Subdivision (a). Rule 26(a)(1)(B) is amended to parallel Rule 34(a) by recognizing that a party must disclose electronically stored information as well as documents that it may use to support its claims or defenses. The term "electronically stored information" has the same broad meaning in Rule 26(a)(1) as in Rule 34(a). This amendment is consistent with the 1993 addition of Rule 26(a)(1)(B). The term "data compilations" is deleted as unnecessary because it is a subset of both documents and electronically stored information.

Changes Made After Publication and Comment. As noted in the introduction [omitted], this provision was not included in the published rule. It is included as a conforming amendment, to make Rule 26(a)(1) consistent with the changes that were included in the published proposals.

[Subdivision (a)(1)(E).] Civil forfeiture actions are added to the list of exemptions from Rule 26(a)(1) disclosure requirements. These actions are governed by new Supplemental Rule G. Disclosure is not likely to be useful.

Subdivision (b)(2). The amendment to Rule 26(b)(2) is designed to address issues raised by difficulties in locating, retrieving, and providing discovery of some electronically stored information. Electronic storage systems often make it easier to locate and retrieve information. These advantages are properly taken into account in determining the reasonable scope of discovery in a particular case. But some sources of electronically stored information can be accessed only with substantial burden and cost. In a particular case, these burdens and costs may make the information on such sources not reasonably accessible.

It is not possible to define in a rule the different types of technological features that may affect the burdens and costs of accessing electronically stored information. Information systems are designed to provide ready access to information used in regular ongoing activities. They also may be designed so as to provide ready access to information that is not regularly used. But a system may retain information on sources that

Appendix B

are accessible only by incurring substantial burdens or costs. Subparagraph (B) is added to regulate discovery from such sources.

Under this rule, a responding party should produce electronically stored information that is relevant, not privileged, and reasonably accessible, subject to the (b)(2)(C) limitations that apply to all discovery. The responding party must also identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing. The identification should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources.

A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence. Whether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible depends on the circumstances of each case. It is often useful for the parties to discuss this issue early in discovery.

The volume of—and the ability to search—much electronically stored information means that in many cases the responding party will be able to produce information from reasonably accessible sources that will fully satisfy the parties' discovery needs. In many circumstances the requesting party should obtain and evaluate the information from such sources before insisting that the responding party search and produce information contained on sources that are not reasonably accessible. If the requesting party continues to seek discovery of information from sources identified as not reasonably accessible, the parties should discuss the burdens and costs of accessing and retrieving the information, the needs that may establish good cause for requiring all or part of the requested discovery even if the information sought is not reasonably accessible, and conditions on obtaining and producing the information that may be appropriate.

If the parties cannot agree whether, or on what terms, sources identified as not reasonably accessible should be searched and discoverable information produced, the issue may be raised either by a motion to compel discovery or by a motion for a protective order. The parties must confer before bringing either motion. If the parties do not resolve the issue and the court must decide, the responding party must show that the identified sources of information are not reasonably accessible because of undue burden or cost. The requesting party may need discovery to test this assertion. Such discovery might take the form of requiring the responding party to conduct a sampling of information contained on the sources identified as not reasonably accessible; allowing some form of inspection of such sources; or taking depositions of witnesses knowledgeable about the responding party's information systems.

Once it is shown that a source of electronically stored information is not reasonably accessible, the requesting party may still obtain discovery by showing good cause, considering the limitations of Rule 26(b)(2)(C) that balance the costs and potential benefits of discovery. The decision whether to require a responding party to search for and produce information that is not reasonably accessible depends not only on the burdens and costs of doing so, but also on whether those burdens and costs can be justified in the circumstances of the case. Appropriate considerations may include: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

The responding party has the burden as to one aspect of the inquiry-whether the identified sources are not reasonably accessible in light of the burdens and costs required to search for, retrieve, and produce whatever responsive information may be found. The requesting party has the burden of showing that its need for the discovery outweighs the burdens and costs of locating, retrieving, and producing the information. In some cases, the court will be able to determine whether the identified sources are not reasonably accessible and whether the requesting party has shown good cause for some or all of the discovery, consistent with the limitations of Rule 26(b)(2)(C), through a single proceeding or presentation. The good-cause determination, however, may be complicated because the court and parties may know little about what information the sources identified as not reasonably accessible might contain, whether it is relevant, or how valuable it may be to the litigation. In such cases, the parties may need some focused discovery, which may include sampling of the sources, to learn more about what burdens and costs are involved in accessing the information, what the information consists of, and how valuable it is for the litigation in light of information that can be obtained by exhausting other opportunities for discovery.

The good-cause inquiry and consideration of the Rule 26(b)(2)(C) limitations are coupled with the authority to set conditions for discovery. The conditions may take the form of limits on the amount, type, or sources of information required to be accessed and produced. The conditions may also include payment by the requesting party of

Appendix **B**

part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible. A requesting party's willingness to share or bear the access costs may be weighed by the court in determining whether there is good cause. But the producing party's burdens in reviewing the information for relevance and privilege may weigh against permitting the requested discovery.

The limitations of Rule 26(b)(2)(C) continue to apply to all discovery of electronically stored information, including that stored on reasonably accessible electronic sources.

Changes Made after Publication and Comment. This recommendation modifies the version of the proposed rule amendment as published. Responding to comments that the published proposal seemed to require identification of information that cannot be identified because it is not reasonably accessible, the rule text was clarified by requiring identification of sources that are not reasonably accessible. The test of reasonable accessibility was clarified by adding "because of undue burden or cost."

The published proposal referred only to a motion by the requesting party to compel discovery. The rule text has been changed to recognize that the responding party may wish to determine its search and potential preservation obligations by moving for a protective order.

The provision that the court may for good cause order discovery from sources that are not reasonably accessible is expanded in two ways. It now states specifically that the requesting party is the one who must show good cause, and it refers to consideration of the limitations on discovery set out in present Rule 26(b)(2)(i), (ii), and (iii).

The published proposal was added at the end of present Rule 26(b)(2). It has been relocated to become a new subparagraph (B), allocating present Rule 26(b)(2) to new subparagraphs (A) and (C). The Committee Note was changed to reflect the rule text revisions. It also was shortened. The shortening was accomplished in part by deleting references to problems that are likely to become antique as technology continues to evolve, and in part by deleting passages that were at a level of detail better suited for a practice manual than a Committee Note.

The changes from the published proposed amendment to Rule 26(b)(2) are set out below. [Omitted]

Subdivision (b)(5). The Committee has repeatedly been advised that the risk of privilege waiver, and the work necessary to avoid it, add to the costs and delay of discov-

Select Federal Rules of Civil Procedure

ery. When the review is of electronically stored information, the risk of waiver, and the time and effort required to avoid it, can increase substantially because of the volume of electronically stored information and the difficulty in ensuring that all information to be produced has in fact been reviewed. Rule 26(b)(5)(A) provides a procedure for a party that has withheld information on the basis of privilege or protection as trial-preparation material to make the claim so that the requesting party can decide whether to contest the claim and the court can resolve the dispute. Rule 26(b)(5)(B) is added to provide a procedure for a party to assert a claim of privilege or trial-preparation material protection after information is produced in discovery in the action and, if the claim is contested, permit any party that received the information to present the matter to the court for resolution.

Rule 26(b)(5)(B) does not address whether the privilege or protection that is asserted after production was waived by the production. The courts have developed principles to determine whether, and under what circumstances, waiver results from inadvertent production of privileged or protected information. Rule 26(b)(5)(B) provides a procedure for presenting and addressing these issues. Rule 26(b)(5)(B) works in tandem with Rule 26(f), which is amended to direct the parties to discuss privilege issues in preparing their discovery plan, and which, with amended Rule 16(b), allows the parties to ask the court to include in an order any agreements the parties reach regarding issues of privilege or trial-preparation material protection. Agreements reached under Rule 26(f)(4) and orders including such agreements entered under Rule 16(b)(6) may be considered when a court determines whether a waiver has occurred. Such agreements and orders ordinarily control if they adopt procedures different from those in Rule 26(b)(5)(B).

A party asserting a claim of privilege or protection after production must give notice to the receiving party. That notice should be in writing unless the circumstances preclude it. Such circumstances could include the assertion of the claim during a deposition. The notice should be as specific as possible in identifying the information and stating the basis for the claim. Because the receiving party must decide whether to challenge the claim and may sequester the information and submit it to the court for a ruling on whether the claimed privilege or protection applies and whether it has been waived, the notice should be sufficiently detailed so as to enable the receiving party and the court to understand the basis for the claim and to determine whether waiver has occurred. Courts will continue to examine whether a claim of privilege or protection was made at a reasonable time when delay is part of the waiver determination under the governing law. After receiving notice, each party that received the information must promptly return, sequester, or destroy the information and any copies it has. The option of sequestering or destroying the information is included in part because the receiving party may have incorporated the information in protected trial-preparation materials. No receiving party may use or disclose the information pending resolution of the privilege claim. The receiving party may present to the court the questions whether the information is privileged or protected as trial-preparation material, and whether the privilege or protection has been waived. If it does so, it must provide the court with the grounds for the privilege or protection specified in the producing party's notice, and serve all parties. In presenting the question, the party may use the content of the information only to the extent permitted by the applicable law of privilege, protection for trial-preparation material, and professional responsibility.

If a party disclosed the information to nonparties before receiving notice of a claim of privilege or protection as trial-preparation material, it must take reasonable steps to retrieve the information and to return it, sequester it until the claim is resolved, or destroy it.

Whether the information is returned or not, the producing party must preserve the information pending the court's ruling on whether the claim of privilege or of protection is properly asserted and whether it was waived. As with claims made under Rule 26(b)(5)(A), there may be no ruling if the other parties do not contest the claim.

Changes Made After Publication and Comment. The rule recommended for approval is modified from the published proposal. The rule is expanded to include trial-preparation protection claims in addition to privilege claims.

The published proposal referred to production "without intending to waive a claim of privilege." This reference to intent was deleted because many courts include intent in the factors that determine whether production waives privilege.

The published proposal required that the producing party give notice "within a reasonable time." The time requirement was deleted because it seemed to implicate the question whether production effected a waiver, a question not addressed by the rule, and also because a receiving party cannot practicably ignore a notice that it believes was unreasonably delayed. The notice procedure was further changed to require that the producing party state the basis for the claim.

Two statements in the published Note have been brought into the rule text. The first provides that the receiving party may not use or disclose the information until the

claim is resolved. The second provides that if the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it.

The rule text was expanded by adding a provision that the receiving party may promptly present the information to the court under seal for a determination of the claim.

The published proposal provided that the producing party must comply with Rule 26(b)(5)(A) after making the claim. This provision was deleted as unnecessary.

Changes are made in the Committee Note to reflect the changes in the rule text.

The changes from the published rule are shown below. [Omitted]

Subdivision (f). Rule 26(f) is amended to direct the parties to discuss discovery of electronically stored information during their discovery-planning conference. The rule focuses on "issues relating to disclosure or discovery of electronically stored information"; the discussion is not required in cases not involving electronic discovery, and the amendment imposes no additional requirements in those cases. When the parties do anticipate disclosure or discovery of electronically stored information, discussion at the outset may avoid later difficulties or ease their resolution.

When a case involves discovery of electronically stored information, the issues to be addressed during the Rule 26(f) conference depend on the nature and extent of the contemplated discovery and of the parties' information systems. It may be important for the parties to discuss those systems, and accordingly important for counsel to become familiar with those systems before the conference. With that information, the parties can develop a discovery plan that takes into account the capabilities of their computer systems. In appropriate cases identification of, and early discovery from, individuals with special knowledge of a party's computer systems may be helpful.

The particular issues regarding electronically stored information that deserve attention during the discovery planning stage depend on the specifics of the given case. See Manual for Complex Litigation (4th) §40.25(2) (listing topics for discussion in a proposed order regarding meet-and-confer sessions). For example, the parties may specify the topics for such discovery and the time period for which discovery will be sought. They may identify the various sources of such information within a party's control that should be searched for electronically stored information. They may discuss whether the information is reasonably accessible to the party that has it, including the burden or cost of retrieving and reviewing the information. See Rule

Appendix B

Essentials of E-Discovery

26(b)(2)(B). Rule 26(f)(3) explicitly directs the parties to discuss the form or forms in which electronically stored information might be produced. The parties may be able to reach agreement on the forms of production, making discovery more efficient. Rule 34(b) is amended to permit a requesting party to specify the form or forms in which it wants electronically stored information produced. If the requesting party does not specify a form, Rule 34(b) directs the responding party to state the forms it intends to use in the production. Early discussion of the forms of production may facilitate the application of Rule 34(b) by allowing the parties to determine what forms of production will meet both parties' needs. Early identification of disputes over the forms of productions using inappropriate forms.

Rule 26(f) is also amended to direct the parties to discuss any issues regarding preservation of discoverable information during their conference as they develop a discovery plan. This provision applies to all sorts of discoverable information, but can be particularly important with regard to electronically stored information. The volume and dynamic nature of electronically stored information may complicate preservation obligations. The ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information. Failure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes.

The parties' discussion should pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities. Complete or broad cessation of a party's routine computer operations could paralyze the party's activities. *Cf. Manual for Complex Litigation* (4th) §11.422 ("A blanket preservation order may be prohibitively expensive and unduly burdensome for parties dependent on computer systems for their day-to-day operations.") The parties should take account of these considerations in their discussions, with the goal of agreeing on reasonable preservation steps.

The requirement that the parties discuss preservation does not imply that courts should routinely enter preservation orders. A preservation order entered over objections should be narrowly tailored. Ex parte preservation orders should issue only in exceptional circumstances.

Rule 26(f) is also amended to provide that the parties should discuss any issues relating to assertions of privilege or of protection as trial-preparation materials, including whether the parties can facilitate discovery by agreeing on procedures for asserting claims of privilege or protection after production and whether to ask the court to enter
Select Federal Rules of Civil Procedure

an order that includes any agreement the parties reach. The Committee has repeatedly been advised about the discovery difficulties that can result from efforts to guard against waiver of privilege and work-product protection. Frequently parties find it necessary to spend large amounts of time reviewing materials requested through discovery to avoid waiving privilege. These efforts are necessary because materials subject to a claim of privilege or protection are often difficult to identify. A failure to withhold even one such item may result in an argument that there has been a waiver of privilege as to all other privileged materials on that subject matter. Efforts to avoid the risk of waiver can impose substantial costs on the party producing the material and the time required for the privilege review can substantially delay access for the party seeking discovery.

These problems often become more acute when discovery of electronically stored information is sought. The volume of such data, and the informality that attends use of e-mail and some other types of electronically stored information, may make privilege determinations more difficult, and privilege review correspondingly more expensive and time consuming. Other aspects of electronically stored information pose particular difficulties for privilege review. For example, production may be sought of information automatically included in electronic files but not apparent to the creator or to readers. Computer programs may retain draft language, editorial comments, and other deleted matter (sometimes referred to as "embedded data" or "embedded edits") in an electronic file but not make them apparent to the reader. Information describing the history, tracking, or management of an electronic file (sometimes called "metadata") is usually not apparent to the reader viewing a hard copy or a screen image. Whether this information should be produced may be among the topics discussed in the Rule 26(f) conference. If it is, it may need to be reviewed to ensure that no privileged information is included, further complicating the task of privilege review.

Parties may attempt to minimize these costs and delays by agreeing to protocols that minimize the risk of waiver. They may agree that the responding party will provide certain requested materials for initial examination without waiving any privilege or protection-sometimes known as a "quick peek." The requesting party then designates the documents it wishes to have actually produced. This designation is the Rule 34 request. The responding party then responds in the usual course, screening only those documents actually requested for formal production and asserting privilege claims as provided in Rule 26(b)(5)(A). On other occasions, parties enter agreements—sometimes called "clawback agreements"—that production without intent to waive privilege or protection should not be a waiver so long as the responding party identifies the documents mistakenly produced, and that the documents should be returned under

those circumstances. Other voluntary arrangements may be appropriate depending on the circumstances of each litigation. In most circumstances, a party who receives information under such an arrangement cannot assert that production of the information waived a claim of privilege or of protection as trial-preparation material.

Although these agreements may not be appropriate for all cases, in certain cases they can facilitate prompt and economical discovery by reducing delay before the discovering party obtains access to documents, and by reducing the cost and burden of review by the producing party. A case-management or other order including such agreements may further facilitate the discovery process. Form 35 is amended to include a report to the court about any agreement regarding protections against inadvertent forfeiture or waiver of privilege or protection that the parties have reached, and Rule 16(b) is amended to recognize that the court may include such an agreement in a case-management or other order. If the parties agree to entry of such an order, their proposal should be included in the report to the court.

Rule 26(b)(5)(B) is added to establish a parallel procedure to assert privilege or protection as trial-preparation material after production, leaving the question of waiver to later determination by the court.

Changes Made After Publication and Comment. The Committee recommends a modified version of what was published. Rule 26(f)(3) was expanded to refer to the form "or forms" of production, in parallel with the like change in Rule 34. Different forms may be suitable for different sources of electronically stored information.

The published Rule 26(f)(4) proposal described the parties' views and proposals concerning whether, on their agreement, the court should enter an order protecting the right to assert privilege after production. This has been revised to refer to the parties' views and proposals concerning any issues relating to claims of privilege, including-if the parties agree on a procedure to assert such claims after production-whether to ask the court to include their agreement in an order. As with Rule 16(b)(6), this change was made to avoid any implications as to the scope of the protection that may be afforded by court adoption of the parties' agreement.

Rule 26(f)(4) also was expanded to include trial-preparation materials.

The Committee Note was revised to reflect the changes in the rule text.

2015 Advisory Committee Notes

Rule 26(b)(1) is changed in several ways.

Information is discoverable under revised Rule 26(b)(1) if it is relevant to any party's claim or defense and is proportional to the needs of the case. The considerations that bear on proportionality are moved from present Rule 26(b)(2)(C)(iii), slightly rearranged and with one addition.

Most of what now appears in Rule 26(b)(2)(C)(iii) was first adopted in 1983. The 1983 provision was explicitly adopted as part of the scope of discovery defined by Rule 26(b)(1). Rule 26(b)(1) directed the court to limit the frequency or extent of use of discovery if it determined that "the discovery is unduly burdensome or expensive, taking into account the needs of the case, the amount in controversy, limitations on the parties' resources, and the importance of the issues at stake in the litigation." At the same time, Rule 26(g) was added. Rule 26(g) provided that signing a discovery request, response, or objection certified that the request, response, or objection was "not unreasonable or unduly burdenscme or expensive, given the needs of the case, the discovery already had in the case, the amount in controversy, and the importance of the issues at stake in the litigation." The parties thus shared the responsibility to honor these limits on the scope of discovery.

The 1983 Committee Note stated that the new provisions were added "to deal with the problem of over-discovery. The objective is to guard against redundant or disproportionate discovery by giving the court authority to reduce the amount of discovery that may be directed to matters that are otherwise proper subjects of inquiry. The new sentence is intended to encourage judges to be more aggressive in identifying and discovery reflect the existing practice of many courts in issuing protective orders under Rule $26(c) \dots$ On the whole, however, district judges have been reluctant to limit the use of the discovery devices."

The clear focus of the 1983 provisions may have been softened, although inadvertently, by the amendments made in 1993. The 1993 Committee Note explained: "[F]ormer paragraph (b)(1) [was] subdivided into two paragraphs for ease of reference and to avoid renumbering of paragraphs (3) and (4)." Subdividing the paragraphs, however, was done in a way that could be read to separate the proportionality provisions as "limitations," no longer an integral part of the (b)(1) scope provisions. That appearance was immediately offset by the next statement in the Note: "Textual

changes are then made in new paragraph (2) to enable the court to keep tighter rein on the extent of discovery."

The 1993 amendments added two factors to the considerations that bear on limiting discovery: whether "the burden or expense of the proposed discovery outweighs its likely benefit," and "the importance of the proposed discovery in resolving the issues." Addressing these and other limitations added by the 1993 discovery amendments, the Committee Note stated that "[t]he revisions in Rule 26(b)(2) are intended to provide the court with broader discretion to impose additional restrictions on the scope and extent of discovery...."

The relationship between Rule 26(b)(1) and (2) was further addressed by an amendment made in 2000 that added a new sentence at the end of (b)(1): "All discovery is subject to the limitations imposed by Rule 26(b)(2)(i), (ii), and (iii)[now Rule 26(b)(2)(C)]." The Committee Note recognized that "[t]hese limitations apply to discovery that is otherwise within the scope of subdivision (b)(1)." It explained that the Committee had been told repeatedly that courts were not using these limitations as originally intended. "This otherwise redundant cross-reference has been added to emphasize the need for active judicial use of subdivision (b)(2) to control excessive discovery."

The present amendment restores the proportionality factors to their original place in defining the scope of discovery. This change reinforces the Rule 26(g) obligation of the parties to consider these factors in making discovery requests, responses, or objections.

Restoring the proportionality calculation to Rule 26(b)(1) does not change the existing responsibilities of the court and the parties to consider proportionality, and the change does not place on the party seeking discovery the burden of addressing all proportionality considerations.

Nor is the change intended to permit the opposing party to refuse discovery simply by making a boilerplate objection that it is not proportional. The parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes.

The parties may begin discovery without a full appreciation of the factors that bear on proportionality. A party requesting discovery, for example, may have little information about the burden or expense of responding. A party requested to provide discovery may have little information about the importance of the discovery in resolving the

issues as understood by the requesting party. Many of these uncertainties should be addressed and reduced in the parties' Rule 26(f) conference and in scheduling and pretrial conferences with the court. But if the parties continue to disagree, the discovery dispute could be brought before the court and the parties' responsibilities would remain as they have been since 1983. A party claiming undue burden or expense ordinarily has far better information—perhaps the only information—with respect to that part of the determination. A party claiming that a request is important to resolve the issues should be able to explain the ways in which the underlying information bears on the issues as that party understands them. The court's responsibility, using all the information provided by the parties, is to consider these and all the other factors in reaching a case-specific determination of the appropriate scope of discovery.

The direction to consider the parties' relative access to relevant information adds new text to provide explicit focus on considerations already implicit in present Rule 26(b)(2)(C)(iii). Some cases involve what often is called "information asymmetry." One party—often an individual plaintiff—may have very little discoverable information. The other party may have vast amounts of information, including information that can be readily retrieved and information that is more difficult to retrieve. In practice these circumstances often mean that the burden of responding to discovery lies heavier on the party who has more information, and properly so.

Restoring proportionality as an express component of the scope of discovery warrants repetition of parts of the 1983 and 1993 Committee Notes that must not be lost from sight. The 1983 Committee Note explained that "[t]he rule contemplates greater judicial involvement in the discovery process and thus acknowledges the reality that it cannot always operate on a self-regulating basis." The 1993 Committee Note further observed that "[t]he information explosion of recent decades has greatly increased both the potential cost of wide-ranging discovery and the potential for discovery to be used as an instrument for delay or oppression." What seemed an explosion in 1993 has been exacerbated by the advent of e-discovery. The present amendment again reflects the need for continuing and close judicial involvement in the cases that do not yield readily to the ideal of effective party management. It is expected that discovery will be effectively managed by the parties in many cases. But there will be important occasions for judicial management, both when the parties are legitimately unable to resolve important differences and when the parties fall short of effective, cooperative management on their own.

It also is important to repeat the caution that the monetary stakes are only one factor, to be balanced against other factors. The 1983 Committee Note recognized "the significance of the substantive issues, as measured in philosophic, social, or institutional terms. Thus the rule recognizes that many cases in public policy spheres, such as employment practices, free speech, and other matters, may have importance far beyond the monetary amount involved." Many other substantive areas also may involve litigation that seeks relatively small amounts of money, or no money at all, but that seeks to vindicate vitally important personal or public values.

So too, consideration of the parties' resources does not foreclose discovery requests addressed to an impecunious party, nor justify unlimited discovery requests addressed to a wealthy party. The 1983 Committee Note cautioned that "[t]he court must apply the standards in an even-handed manner that will prevent use of discovery to wage a war of attrition or as a device to coerce a party, whether financially weak or affluent."

The burden or expense of proposed discovery should be determined in a realistic way. This includes the burden or expense of producing electronically stored information. Computer-based methods of searching such information continue to develop, particularly for cases involving large volumes of electronically stored information. Courts and parties should be willing to consider the opportunities for reducing the burden or expense of discovery as reliable means of searching electronically stored information become available.

A portion of present Rule 26(b)(1) is omitted from the proposed revision. After allowing discovery of any matter relevant to any party's claim or defense, the present rule adds: "including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter." Discovery of such matters is so deeply entrenched in practice that it is no longer necessary to clutter the long text of Rule 26 with these examples. The discovery identified in these examples should still be permitted under the revised rule when relevant and proportional to the needs of the case. Framing intelligent requests for electronically stored information, for example, may require detailed information about another party's information systems and other information resources.

The amendment deletes the former provision authorizing the court, for good cause, to order discovery of any matter relevant to the subject matter involved in the action. The Committee has been informed that this language is rarely invoked. Proportional discovery relevant to any party's claim or defense suffices, given a proper understanding of what is relevant to a claim or defense. The distinction between matter relevant to a claim or defense and matter relevant to the subject matter was introduced in 2000. The 2000 Note offered three examples of information that, suitably focused, would be relevant to the parties' claims or defenses. The examples were "other incidents of the

Select Federal Rules of Civil Procedure

same type, or involving the same product"; "information about organizational arrangements or filing systems"; and "information that could be used to impeach a likely witness." Such discovery is not foreclosed by the amendments. Discovery that is relevant to the parties' claims or defenses may also support amendment of the pleadings to add a new claim or defense that affects the scope of discovery.

The former provision for discovery of relevant but inadmissible information that appears "reasonably calculated to lead to the discovery of admissible evidence" is also deleted. The phrase has been used by some, incorrectly, to define the scope of discovery. As the Committee Note to the 2000 amendments observed, use of the "reasonably calculated" phrase to define the scope of discovery "might swallow any other limitation on the scope of discovery." The 2000 amendments sought to prevent such misuse by adding the word "Relevant" at the beginning of the sentence, making clear that "relevant' means within the scope of discovery as defined in this subdivision …" The "reasonably calculated" phrase has continued to create problems, however, and is removed by these amendments. It is replaced by the direct statement that "Information within this scope of discovery need not be admissible in evidence to be discoverable." Discovery of nonprivileged information not admissible in evidence remains available so long as it is otherwise within the scope of discovery.

Rule 26(b)(2)(C)(iii) is amended to reflect the transfer of the considerations that bear on proportionality to Rule 26(b)(1). The court still must limit the frequency or extent of proposed discovery, on motion or on its own, if it is outside the scope permitted by Rule 26(b)(1).

Rule 26(c)(1)(B) is amended to include an express recognition of protective orders that allocate expenses for disclosure or discovery. Authority to enter such orders is included in the present rule, and courts already exercise this authority. Explicit recognition will forestall the temptation some parties may feel to contest this authority. Recognizing the authority does not imply that cost-shifting should become a common practice. Courts and parties should continue to assume that a responding party ordinarily bears the costs of responding.

Rule 26(d)(2) is added to allow a party to deliver Rule 34 requests to another party more than 21 days after that party has been served even though the parties have not yet had a required Rule 26(f) conference. Delivery may be made by any party to the party that has been served, and by that party to any plaintiff and any other party that has been served. Delivery does not count as service; the requests are considered to be served at the first Rule 26(f) conference. Under Rule 34(b)(2)(A) the time to respond runs from service. This relaxation of the discovery moratorium is designed to facili-

tate focused discussion during the Rule 26(f) conference. Discussion at the conference may produce changes in the requests. The opportunity for advance scrutiny of requests delivered before the Rule 26(f) conference should not affect a decision whether to allow additional time to respond.

Rule 26(d)(3) is renumbered and amended to recognize that the parties may stipulate to case-specific sequences of discovery.

Rule 26(f)(3) is amended in parallel with Rule 16(b)(3) to add two items to the discovery plan—issues about preserving electronically stored information and court orders under Evidence Rule 502.

Rule 34—Producing Documents, Electronically Stored Information, and Tangible Things, or Entering Onto Land, for Inspection and Other Purposes

- (a) *In General*. A party may serve on any other party a request within the scope of Rule 26(b):
 - (1) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control:
 - (A) any designated documents or electronically stored informationincluding writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form; or
 - (B) any designated tangible things; or
 - (2) to permit entry onto designated land or other property possessed or controlled by the responding party, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.
- (b) Procedure.
 - (1) Contents of the Request. The request:
 - (A) must describe with reasonable particularity each item or category of items to be inspected;

- (B) must specify a reasonable time, place, and manner for the inspection and for performing the related acts; and
- (C) may specify the form or forms in which electronically stored information is to be produced.
- (2) Responses and Objections.
 - (A) Time to Respond. The party to whom the request is directed must respond in writing within 30 days after being served or-if the request was delivered under Rule 26(d)(2)—within 30 days after the parties' first Rule 26(f) conference. A shorter or longer time may be stipulated to under Rule 29 or be ordered by the court.
 - (B) Responding to Each Item. For each item or category, the response must either state that inspection and related activities will be permitted as requested or state with specificity the grounds for objecting to the request, including the reasons. The responding party may state that it will produce copies of documents or of electronically stored information instead of permitting inspection. The production must then be completed no later than the time for inspection specified in the request or another reasonable time specified in the response.
 - (C) Objections. An objection must state whether any responsive materials are being withheld on the basis of that objection. An objection to part of a request must specify the part and permit inspection of the rest.
 - (D) Responding to a Request for Production of Electronically Stored Information. The response may state an objection to a requested form for producing electronically stored information. If the responding party cbjects to a requested form—or if no form was specified in the recuest—the party must state the form or forms it intends to use.
 - (E) Producing the Documents or Electronically Stored Information. Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:
 - A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;

- (ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and
- (iii) A party need not produce the same electronically stored information in more than one form.
- (c) *Nonparties.* As provided in Rule 45, a nonparty may be compelled to produce documents and tangible things or to permit an inspection.

2006 Advisory Committee Notes

Subdivision (a). As originally adopted, Rule 34 focused on discovery of "documents" and "things." In 1970, Rule 34(a) was amended to include discovery of data compilations, anticipating that the use of computerized information would increase. Since then, the growth in electronically stored information and in the variety of systems for creating and storing such information has been dramatic. Lawyers and judges interpreted the term "documents" to include electronically stored information because it was obviously improper to allow a party to evade discovery obligations on the basis that the label had not kept pace with changes in information technology. But it has become increasingly difficult to say that all forms of electronically stored information, many dynamic in nature, fit within the traditional concept of a "document." Electronically stored information may exist in dynamic databases and other forms far different from fixed expression on paper. Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents. The change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined. At the same time, a Rule 34 request for production of "documents" should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and "documents."

Discoverable information often exists in both paper and electronic form, and the same or similar information might exist in both. The items listed in Rule 34(a) show different ways in which information may be recorded or stored. Images, for example, might be hard-copy documents or electronically stored information. The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. Rule 34(a)(1) is expansive and includes any type of information that is stored electronically. A common example often sought in discovery is electronic communications, such as e-mail. The rule covers—either as documents or as electronically stored information—information "stored in any medium," to encompass future developments in computer technology. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.

References elsewhere in the rules to "electronically stored information" should be understood to invoke this expansive approach. A companion change is made to Rule 33(d), making it explicit that parties choosing to respond to an interrogatory by permitting access to responsive records may do so by providing access to electronically stored information. More generally, the term used in Rule 34(a)(1) appears in a number of other amendments, such as those to Rules 26(a)(1), 26(b)(2), 26(b)(5)(B), 26(f), 34(b), 37(f), and 45. In each of these rules, electronically stored information has the same broad meaning it has under Rule 34(a)(1). References to "documents" appear in discovery rules that are not amended, including Rules 30(f), 36(a), and 37(c)(2). These references should be interpreted to include electronically stored information as circumstances warrant.

The term "electronically stored information" is broad, but whether material that falls within this term should be produced, and in what form, are separate questions that must be addressed under Rules 26(b), 26(c), and 34(b).

The Rule 34(a) requirement that, if necessary, a party producing electronically stored information translate it into reasonably usable form does not address the issue of translating from one human language to another. See In re Puerto Rico Elect. Power Auth., 687 F.2d 501, 504–510 (1st Cir. 1989).

Rule 34(a)(1) is also amended to make clear that parties may request an opportunity to test or sample materials sought under the rule in addition to inspecting and copying them. That opportunity may be important for both electronically stored information and hard-copy materials. The current rule is not clear that such testing or sampling is authorized; the amendment expressly permits it. As with any other form of discovery, issues of burden and intrusiveness raised by requests to test or sample can be addressed under Rules 26(b)(2) and 26(c). Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.

Rule 34(a)(1) is further amended to make clear that tangible things must—like documents and land sought to be examined—be designated in the request.

Subdivision (b). Rule 34(b) provides that a party must produce documents as they are kept in the usual course of business or must organize and label them to correspond with the categories in the discovery request. The production of electronically stored information should be subject to comparable requirements to protect against deliberate or inadvertent production in ways that raise unnecessary obstacles for the requesting party. Rule 34(b) is amended to ensure similar protection for electronically stored information.

The amendment to Rule 34(b) permits the requesting party to designate the form or forms in which it wants electronically stored information produced. The form of production is more important to the exchange of electronically stored information than of hard-copy materials, although a party might specify hard copy as the requested form. Specification of the desired form or forms may facilitate the orderly, efficient, and cost-effective discovery of electronically stored information. The rule recognizes that different forms of production may be appropriate for different types of electronically stored information. Using current technology, for example, a party might be called upon to produce word processing documents, e-mail messages, electronic spread-sheets, different image or sound files, and material from databases. Requiring that such diverse types of electronically stored information all be produced in the same form could prove impossible, and even if possible could increase the cost and burdens of producing and using the information. The rule therefore provides that the requesting party may ask for different forms of production for different types of electronically stored information.

The rule does not require that the requesting party choose a form or forms of production. The requesting party may not have a preference. In some cases, the requesting party may not know what form the producing party uses to maintain its electronically stored information, although Rule 26(f)(3) is amended to call for discussion of the form of production in the parties' prediscovery conference.

The responding party also is involved in determining the form of production. In the written response to the production request that Rule 34 requires, the responding party must state the form it intends to use for producing electronically stored information if the requesting party does not specify a form or if the responding party objects to a form that the requesting party specifies. Stating the intended form before the production occurs may permit the parties to identify and seek to resolve disputes before the expense and work of the production occurs. A party that responds to a discovery

request by simply producing electronically stored information in a form of its choice, without identifying that form in advance of the production in the response required by Rule 34(b), runs a risk that the requesting party can show that the produced form is not reasonably usable and that it is entitled to production of some or all of the information in an additional form. Additional time might be required to permit a responding party to assess the appropriate form or forms of production.

If the requesting party is not satisfied with the form stated by the responding party, or if the responding party has objected to the form specified by the requesting party, the parties must meet and confer under Rule 37(a)(2)(B) in an effort to resolve the matter before the requesting party can file a motion to compel. If they cannot agree and the court resolves the dispute, the court is not limited to the forms initially chosen by the requesting party, stated by the responding party, or specified in this rule for situations in which there is no court order or party agreement.

If the form of production is not specified by party agreement or court order, the responding party must produce electronically stored information either in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable. Rule 34(a) requires that, if necessary, a responding party "translate" information it produces into a "reasonably usable" form. Under some circumstances, the responding party may need to provide some reasonable amount of technical support, information on application software, or other reasonable assistance to enable the requesting party to use the information. The rule does not require a party to produce electronically stored information in the form it [sic] which it is ordinarily maintained, as long as it is produced in a reasonably usable form. But the option to produce in a reasonably usable form does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information efficiently in the litigation. If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature.

Some electronically stored information may be ordinarily maintained in a form that is not reasonably usable by any party. One example is "legacy" data that can be used only by superseded systems. The questions whether a producing party should be required to convert such information to a more usable form, or should be required to produce it at all, should be addressed under Rule 26(b)(2)(B).

Whether or not the requesting party specified the form of production, Rule 34(b) provides that the same electronically stored information ordinarily be produced in only one form.

Changes Made after Publication and Comment. The proposed amendment recommended for approval has been modified from the published version. The sequence of "documents or electronically stored information" is changed to emphasize that the parenthetical exemplifications apply equally to illustrate "documents" and "electronically stored information." The reference to "detection devices" is deleted as redundant with "translated" and as archaic.

The references to the form of production are changed in the rule and Committee Note to refer also to "forms." Different forms may be appropriate or necessary for different sources of information.

The published proposal allowed the requesting party to specify a form for production and recognized that the responding party could object to the requested form. This procedure is now amplified by directing that the responding party state the form or forms it intends to use for production if the request does not specify a form or if the responding party objects to the requested form.

The default forms of production to be used when the parties do not agree on a form and there is no court order are changed in part. As in the published proposal, one default form is "a form or forms in which [electronically stored information] is ordinarily maintained." The alternative default form, however, is changed from "an electronically searchable form" to "a form or forms that are reasonably usable." "[A]n electronically searchable form" proved to have several defects. Some electronically stored information cannot be searched electronically. In addition, there often are many different levels of electronic searchability—the published default would authorize production in a minimally searchable form even though more easily searched forms might be available at equal or less cost to the responding party.

The provision that absent court order a party need not produce the same electronically stored information in more than one form was moved to become a separate item for the sake of emphasis.

The Committee Note was changed to reflect these changes in rule text, and also to clarify many aspects of the published Note. In addition, the Note was expanded to add a caveat to the published amendment that establishes the rule that documents—and now electronically stored information—may be tested and sampled as well as inspected and copied. Fears were expressed that testing and sampling might imply routine direct access to a party's information system. The Note states that direct access is not a routine right, "although such access might be justified in some circumstances."

2015 Advisory Committee Notes

Several amendments are made in Rule 34, aimed at reducing the potential to impose unreasonable burdens by objections to requests to produce.

Rule 34(b)(2)(A) is amended to fit with new Rule 26(d)(2). The time to respond to a Rule 34 request delivered before the parties' Rule 26(f) conference is 30 days after the first Rule 26(f) conference.

Rule 34(b)(2)(B) is amended to require that objections to Rule 34 requests be stated with specificity. This provision adopts the language of Rule 33(b)(4), eliminating any doubt that less specific objections might be suitable under Rule 34. The specificity of the objection ties to the new provision in Rule 34(b)(2)(C) directing that an objection must state whether any responsive materials are being withheld on the basis of that objection. An objection may state that a request is overbroad, but if the objection recognizes that some part of the request is appropriate the objection should state the scope that is not overbroad. Examples would be a statement that the responding party will limit the search to documents or electronically stored information created within a given period of time prior to the events in suit, or to specified sources. When there is such an objection, the statement of what has been withheld can properly identify as matters "withheld" anything beyond the scope of the search specified in the objection.

Rule 34(b)(2)(B) is further amended to reflect the common practice of producing copies of documents or electronically stored information rather than simply permitting inspection. The response to the request must state that copies will be produced. The production must be completed either by the time for inspection specified in the request or by another reasonable time specifically identified in the response. When it is necessary to make the production in stages the response should specify the beginning and end dates of the production.

Rule 34(b)(2)(C) is amended to provide that an objection to a Rule 34 request must state whether anything is being withheld on the basis of the objection. This amendment should end the confusion that frequently arises when a producing party states several objections and still produces information, leaving the requesting party uncertain whether any relevant and responsive information has been withheld on the basis of the objections. The producing party does not need to provide a detailed description or log of all documents withheld, but does need to alert other parties to the fact that documents have been withheld and thereby facilitate an informed discussion of the objection. An objection that states the limits that have controlled the search for responsive and relevant materials qualifies as a statement that the materials have been "withheld."

Rule 37—Failure to Make Disclosures or to Cooperate in Discovery; Sanctions

- (a) Motion for an Order Compelling Disclosure or Discovery.
 - (1) In General. On notice to other parties and all affected persons, a party may move for an order compelling disclosure or discovery. The motion must include a certification that the movant has in good faith conferred or attempted to confer with the person or party failing to make disclosure or discovery in an effort to obtain it without court action.
 - (2) Appropriate Court. A motion for an order to a party must be made in the court where the action is pending. A motion for an order to a nonparty must be made in the court where the discovery is or will be taken.
 - (3) Specific Motions.
 - (A) To Compel Disclosure. If a party fails to make a disclosure required by Rule 26(a), any other party may move to compel disclosure and for appropriate sanctions.
 - (B) To Compel a Discovery Response. A party seeking discovery may move for an order compelling an answer, designation, production, or inspection. This motion may be made if:
 - (i) a deponent fails to answer a question asked under Rule 30 or 31;
 - (ii) a corporation or other entity fails to make a designation under Rule 30(b)(6) or 31(a)(4);
 - (iii) a party fails to answer an interrogatory submitted under Rule 33; or
 - (iv) a party fails to produce documents or fails to respond that

inspection will be permitted—or fails to permit inspection—as requested under Rule 34.

- (C) Related to a Deposition. When taking an oral deposition, the party asking a question may complete or adjourn the examination before moving for an order.
- (4) Evasive or Incomplete Disclosure, Answer, or Response. For purposes of this subdivision (a), an evasive or incomplete disclosure, answer, or response must be treated as a failure to disclose, answer, or respond.
- (5) Payment of Expenses; Protective Orders.
 - (A) If the Motion Is Granted (or Disclosure or Discovery Is Provided After Filing). If the motion is granted—or if the disclosure or requested discovery is provided after the motion was filed—the court must, after giving an opportunity to be heard, require the party or deponent whose conduct necessitated the motion, the party or attorney advising that conduct, or both to pay the movant's reasonable expenses incurred in making the motion, including attorney's fees. But the court must not order this payment if:
 - (i) the movant filed the motion before attempting in good faith to obtain the disclosure or discovery without court action;
 - (ii) the opposing party's nondisclosure, response, or objection was substantially justified; or
 - (iii) other circumstances make an award of expenses unjust.
 - (B) If the Motion Is Denied. If the motion is denied, the court may issue any protective order authorized under Rule 26(c) and must, after giving an opportunity to be heard, require the movant, the attorney filing the motion, or both to pay the party or deponent who opposed the motion its reasonable expenses incurred in opposing the motion, including attorney's fees. But the court must not order this payment if the motion was substantially justified or other circumstances make an award of expenses unjust.
 - (C) If the Motion Is Granted in Part and Denied in Part. If the motion is granted in part and denied in part, the court may issue any protective order authorized under Rule 26(c) and may, after giving

an opportunity to be heard, apportion the reasonable expenses for the motion.

- (b) Failure to Comply with a Court Order.
 - (1) Sanctions Sought in the District Where the Deposition Is Taken. If the court where the discovery is taken orders a deponent to be sworn or to answer a question and the deponent fails to obey, the failure may be treated as contempt of court. If a depositionrelated motion is transferred to the court where the action is pending, and that court orders a deponent to be sworn or to answer a question and the deponent fails to obey, the failure may be treated as contempt of either the court where the discovery is taken or the court where the action is pending.
 - (2) Sanctions Sought in the District Where the Action Is Pending.
 - (A) For Not Obeying a Discovery Order. If a party or a party's officer, director, or managing agent—or a witness designated under Rule 30(b)(6) or 31(a)(4)—fails to obey an order to provide or permit discovery, including an order under Rule 26(f), 35, or 37(a), the court where the action is pending may issue further just orders. They may include the following:
 - directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims;
 - (ii) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence;
 - (iii) striking pleadings in whole or in part;
 - (iv) staying further proceedings until the order is obeyed;
 - (v) dismissing the action or proceeding in whole or in part;
 - (vi) rendering a default judgment against the disobedient party; or
 - (vii) treating as contempt of court the failure to obey any order except an order to submit to a physical or mental examination.
 - (B) For Not Producing a Person for Examination. If a party fails to

comply with an order under Rule 35(a) requiring it to produce another person for examination, the court may issue any of the orders listed in Rule 37(b)(2)(A)(i)-(vi), unless the disobedient party shows that it cannot produce the other person.

- (C) Payment of Expenses. Instead of or in addition to the orders above, the court must order the disobedient party, the attorney advising that party, or both to pay the reasonable expenses, including attorney's fees, caused by the failure, unless the failure was substantially justified or other circumstances make an award of expenses unjust.
- (c) Failure to Disclose, to Supplement an Earlier Response, or to Admit.
 - (1) Failure to Disclose or Supplement. If a party fails to provide information or identify a witness as required by Rule 26(a) or (e), the party is not allowed to use that information or witness to supply evidence on a motion, at a hearing, or at a trial, unless the failure was substantially justified or is harmless. In addition to or instead of this sanction, the court, on motion and after giving an opportunity to be heard:
 - (A) may order payment of the reasonable expenses, including attorney's fees, caused by the failure;
 - (B) may inform the jury of the party's failure; and
 - (C) may impose other appropriate sanctions, including any of the orders listed in Rule 37(b)(2)(A)(i)-(vi).
 - (2) Failure to Admit. If a party fails to admit what is requested under Rule 36 and if the requesting party later proves a document to be genuine or the matter true, the requesting party may move that the party who failed to admit pay the reasonable expenses, including attorney's fees, incurred in making that proof. The court must so order unless:
 - (A) the request was held objectionable under Rule 36(a);
 - (B) the admission sought was of no substantial importance;
 - (C) the party failing to admit had a reasonable ground to believe that it might prevail on the matter; or
 - (D) there was other good reason for the failure to admit.

- (d) Party's Failure to Attend Its Own Deposition, Serve Answers to Interrogatories, or Respond to a Request for Inspection.
 - (1) In General.
 - (A) Motion; Grounds for Sanctions. The court where the action is pending may, on motion, order sanctions if:
 - (i) a party or a party's officer, director, or managing agent—or a person designated under Rule 30(b)(6) or 31(a)(4)—fails, after being served with proper notice, to appear for that person's deposition; or
 - (ii) a party, after being properly served with interrogatories under Rule 33 or a request for inspection under Rule 34, fails to serve its answers, objections, or written response.
 - (B) Certification. A motion for sanctions for failing to answer or respond must include a certification that the movant has in good faith conferred or attempted to confer with the party failing to act in an effort to obtain the answer or response without court action.
 - (2) Unacceptable Excuse for Failing to Act. A failure described in Rule 37(d)(1)(A) is not excused on the ground that the discovery sought was objectionable, unless the party failing to act has a pending motion for a protective order under Rule 26(c).
 - (3) Types of Sanctions. Sanctions may include any of the orders listed in Rule 37(b)(2)(A)(i)-(vi). Instead of or in addition to these sanctions, the court must require the party failing to act, the attorney advising that party, or both to pay the reasonable expenses, including attorney's fees, caused by the failure, unless the failure was substantially justified or other circumstances make an award of expenses unjust.
- (e) *Failure to Preserve Electronically Stored Information*. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
 - (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

- (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
 - (A) presume that the lost information was unfavorable to the party;
 - (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
 - (C) dismiss the action or enter a default judgment.
- (f) Failure to Participate in Framing a Discovery Plan. If a party or its attorney fails to participate in good faith in developing and submitting a proposed discovery plan as required by Rule 26(f), the court may, after giving an opportunity to be heard, require that party or attorney to pay to any other party the reasonable expenses, including attorney's fees, caused by the failure.

2006 Advisory Committee Notes

Subdivision (f). Subdivision (f) is new. It focuses on a distinctive feature of computer operations, the routine alteration and deletion of information that attends ordinary use. Many steps essential to computer operation may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation. As a result, the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part. Under Rule 37(f), absent exceptional circumstances, sanctions cannot be imposed for loss of electronically stored information resulting from the routine, good-faith operation of an electronic information system.

Rule 37(f) applies only to information lost due to the "routine operation of an electronic information system"—the ways in which such systems are generally designed, programmed, and implemented to meet the party's technical and business needs. The "routine operation" of computer systems includes the alteration and overwriting of information, often without the operator's specific direction or awareness, a feature with no direct counterpart in hard-copy documents. Such features are essential to the operation of electronic information systems.

Rule 37(f) applies to information lost due to the routine operation of an information system only if the operation was in good faith. Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation. A preservation obligation may arise

from many sources, including common law, statutes, regulations, or a court order in the case. The good faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold." Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information.

Whether good faith would call for steps to prevent the loss of information on sources that the party believes are not reasonably accessible under Rule 26(b)(2) depends on the circumstances of each case. One factor is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.

The protection provided by Rule 37(f) applies only to sanctions "under these rules." It does not affect other sources of authority to impose sanctions or rules of professional responsibility.

This rule restricts the imposition of "sanctions." It does not prevent a court from making the kinds of adjustments frequently used in managing discovery if a party is unable to provide relevant responsive information. For example, a court could order the responding party to produce an additional witness for deposition, respond to additional interrogatories, or make similar attempts to provide substitutes or alternatives for some or all of the lost information.

Changes Made after Publication and Comment. The published rule barred sanctions only if the party who lost electronically stored information took reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action. A footnote invited comment on an alternative standard that barred sanctions unless the party recklessly or intentionally failed to preserve the information. The present proposal establishes an intermediate standard, protecting against sanctions if the information was lost in the "good faith" operation of an electronic information system. The present proposal carries forward a related element that was a central part of the published proposal—the information must have been lost in the system's "routine operation." The change to a good-faith test made it possible to eliminate the reference to information "discoverable in the action," removing a poten-

Select Federal Rules of Civil Procedure

tial source of confusion as to the duty to preserve information on sources that are identified as not reasonably accessible under Rule 26(b)(2)(B).

The change to a good-faith standard is accompanied by addition of a provision that permits sanctions for loss of information in good- faith routine operation in "exceptional circumstances." This provision recognizes that in some circumstances a court should provide remedies to protect an entirely innocent party requesting discovery against serious prejudice arising from the loss of potentially important information.

As published, the rule included an express exception that denied protection if a party "violated an order in the action requiring it to preserve electronically stored information." This exception was deleted for fear that it would invite routine applications for preservation orders, and often for overbroad orders. The revised Committee Note observes that violation of an order is an element in determining whether a party acted in good faith.

The revised proposal broadens the rule's protection by applying to operation of "an" electronic information system, rather than "the party's" system. The change protects a party who has contracted with an outside firm to provide electronic information storage, avoiding potential arguments whether the system can be characterized as "the party's." The party remains obliged to act in good faith to avoid loss of information in routine operations conducted by the outside firm.

2015 Advisory Committee Notes

Subdivision (a). Rule 37(a)(3)(B)(iv) is amended to reflect the common practice of producing copies of documents or electronically stored information rather than simply permitting inspection. This change brings item (iv) into line with paragraph (B), which provides a motion for an order compelling "production, or inspection."

Subdivision (e). Present Rule 37(e), adopted in 2006, provides: "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, goodfaith operation of an electronic information system." This limited rule has not adequately addressed the serious problems resulting from the continued exponential growth in the volume of such information. Federal circuits have established significantly different standards for imposing sanctions or curative measures on parties who fail to preserve electronically stored information. These developments have caused litigants to expend excessive effort and money on preservation in order to avoid the risk of severe sanctions if a court finds they did not do enough.

New Rule 37(e) replaces the 2006 rule. It authorizes and specifies measures a court may employ if information that should have been preserved is lost, and specifies the findings necessary to justify these measures. It therefore forecloses reliance on inherent authority or state law to determine when certain measures should be used. The rule does not affect the validity of an independent tort claim for spoliation if state law applies in a case and authorizes the claim.

The new rule applies only to electronically stored information, also the focus of the 2006 rule. It applies only when such information is lost. Because electronically stored information often exists in multiple locations, loss from one source may often be harmless when substitute information can be found elsewhere.

The new rule applies only if the lost information should have been preserved in the anticipation or conduct of litigation and the party failed to take reasonable steps to preserve it. Many court decisions hold that potential litigants have a duty to preserve relevant information when litigation is reasonably foreseeable. Rule 37(e) is based on this common-law duty; it does not attempt to create a new duty to preserve. The rule does not apply when information is lost before a duty to preserve arises.

In applying the rule, a court may need to decide whether and when a duty to preserve arose. Courts should consider the extent to which a party was on notice that litigation was likely and that the information would be relevant. A variety of events may alert a party to the prospect of litigation. Often these events provide only limited information about that prospective litigation, however, so that the scope of information that should be preserved may remain uncertain. It is important not to be blinded to this reality by hindsight arising from familiarity with an action as it is actually filed.

Although the rule focuses on the common-law obligation to preserve in the anticipation or conduct of litigation, courts may sometimes consider whether there was an independent requirement that the lost information be preserved. Such requirements arise from many sources—statutes, administrative regulations, an order in another case, or a party's own information-retention protocols. The court should be sensitive, however, to the fact that such independent preservation requirements may be addressed to a wide variety of concerns unrelated to the current litigation. The fact that a party had an independent obligation to preserve information does not necessarily mean that it had such a duty with respect to the litigation, and the fact that the party failed to observe some other preservation obligation does not itself prove that its efforts to preserve were not reasonable with respect to a particular case. The duty to preserve may in some instances be triggered or clarified by a court order in the case. Preservation orders may become more common, in part because Rules 16(b)(3)(B)(iii) and 26(f)(3)(C) are amended to encourage discovery plans and orders that address preservation. Once litigation has commenced, if the parties cannot reach agreement about preservation issues, promptly seeking judicial guidance about the extent of reasonable preservation may be important.

The rule applies only if the information was lost because the party failed to take reasonable steps to preserve the information. Due to the ever-increasing volume of electronically stored information and the multitude of devices that generate such information, perfection in preserving all relevant electronically stored information is often impossible. As under the current rule, the routine, good-faith operation of an electronic information system would be a relevant factor for the court to consider in evaluating whether a party failed to take reasonable steps to preserve lost information, although the prospect of litigation may call for reasonable steps to preserve information by intervening in that routine operation. This rule recognizes that "reasonable steps" to preserve suffice; it does not call for perfection. The court should be sensitive to the party's sophistication with regard to litigation in evaluating preservation efforts; some litigants, particularly individual litigants, may be less familiar with preservation obligations than others who have considerable experience in litigation.

Because the rule calls only for reasonable steps to preserve, it is inapplicable when the loss of information occurs despite the party's reasonable steps to preserve. For example, the information may not be in the party's control. Or information the party has preserved may be destroyed by events outside the party's control—the computer room may be flooded, a "cloud" service may fail, a malign software attack may disrupt a storage system, and so on. Courts may, however, need to assess the extent to which a party knew of and protected against such risks.

Another factor in evaluating the reasonableness of preservation efforts is proportionality. The court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts. A party may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms. It is important that counsel become familiar with their clients' information systems and digital data—including social media—to address these issues. A party urging that preservation requests are disproportionate may need to provide specifics about these matters in order to enable meaningful discussion of the appropriate preservation regime.

Essentials of E-Discovery

When a party fails to take reasonable steps to preserve electronically stored information that should have been preserved in the anticipation or conduct of litigation, and the information is lost as a result, Rule 37(e) directs that the initial focus should be on whether the lost information can be restored or replaced through additional discovery. Nothing in the rule limits the court's powers under Rules 16 and 26 to authorize additional discovery. Orders under Rule 26(b)(2)(B) regarding discovery from sources that would ordinarily be considered inaccessible or under Rule 26(c)(1)(B) on allocation of expenses may be pertinent to solving such problems. If the information is restored or replaced, no further measures should be taken. At the same time, it is important to emphasize that efforts to restore or replace lost information through discovery should be proportional to the apparent importance of the lost information to claims or defenses in the litigation. For example, substantial measures should not be employed to restore or replace information that is marginally relevant or duplicative.

Subdivision (e)(1). This subdivision applies only if information should have been preserved in the anticipation or conduct of litigation, a party failed to take reasonable steps to preserve the information, information was lost as a result, and the information could not be restored or replaced by additional discovery. In addition, a court may resort to (e)(1) measures only "upon finding prejudice to another party from loss of the information." An evaluation of prejudice from the loss of information necessarily includes an evaluation of the information's importance in the litigation.

The rule does not place a burden of proving or disproving prejudice on one party or the other. Determining the content of lost information may be a difficult task in some cases, and placing the burden of proving prejudice on the party that did not lose the information may be unfair. In other situations, however, the content of the lost information may be fairly evident, the information may appear to be unimportant, or the abundance of preserved information may appear sufficient to meet the needs of all parties. Requiring the party seeking curative measures to prove prejudice may be reasonable in such situations. The rule leaves judges with discretion to determine how best to assess prejudice in particular cases.

Once a finding of prejudice is made, the court is authorized to employ measures "no greater than necessary to cure the prejudice." The range of such measures is quite broad if they are necessary for this purpose. There is no all-purpose hierarchy of the severity of various measures; the severity of given measures must be calibrated in terms of their effect on the particular case. But authority to order measures no greater than necessary to cure prejudice does not require the court to adopt measures to cure every possible prejudicial effect. Much is entrusted to the court's discretion.

Select Federal Rules of Civil Procedure

In an appropriate case, it may be that serious measures are necessary to cure prejudice found by the court, such as forbidding the party that failed to preserve information from putting on certain evidence, permitting the parties to present evidence and argument to the jury regarding the loss of information, or giving the jury instructions to assist in its evaluation of such evidence or argument, other than instructions to which subdivision (e)(2) applies. Care must be taken, however, to ensure that curative measures under subdivision (e)(1) do not have the effect of measures that are permitted under subdivision (e)(2) only on a finding of intent to deprive another party of the lost information's use in the litigation. An example of an inappropriate (e)(1) measure might be an order striking pleadings related to, or precluding a party from offering any evidence in support of, the central or only claim or defense in the case. On the other hand, it may be appropriate to exclude a specific item of evidence to offset prejudice caused by failure to preserve other evidence that might contradict the excluded item of evidence.

Subdivision (e)(2). This subdivision authorizes courts to use specified and very severe measures to address or deter failures to preserve electronically stored information, but only on finding that the party that lost the information acted with the intent to deprive another party of the information's use in the litigation. It is designed to provide a uniform standard in federal court for use of these serious measures when addressing failure to preserve electronically stored information. It rejects cases such as *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99 (2d Cir. 2002), that authorize the giving of adverse-inference instructions on a finding of negligence or gross negligence.

Adverse-inference instructions were developed on the premise that a party's intentional loss or destruction of evidence to prevent its use in litigation gives rise to a reasonable inference that the evidence was unfavorable to the party responsible for loss or destruction of the evidence. Negligent or even grossly negligent behavior does not logically support that inference. Information lost through negligence may have been favorable to either party, including the party that lost it, and inferring that it was unfavorable to that party may tip the balance at trial in ways the lost information never would have. The better rule for the negligent or grossly negligent loss of electronically stored information is to preserve a broad range of measures to cure prejudice caused by its loss, but to limit the most severe measures to instances of intentional loss or destruction.

Similar reasons apply to limiting the court's authority to presume or infer that the lost information was unfavorable to the party who lost it when ruling on a pretrial motion or presiding at a bench trial. Subdivision (e)(2) limits the ability of courts to draw

adverse inferences based on the loss of information in these circumstances, permitting them only when a court finds that the information was lost with the intent to prevent its use in litigation.

Subdivision (e)(2) applies to jury instructions that permit or require the jury to presume or infer that lost information was unfavorable to the party that lost it. Thus, it covers any instruction that directs or permits the jury to infer from the loss of information that it was in fact unfavorable to the party that lost it. The subdivision does not apply to jury instructions that do not involve such an inference. For example, subdivision (e)(2) would not prohibit a court from allowing the parties to present evidence to the jury concerning the loss and likely relevance of information and instructing the jury that it may consider that evidence, along with all the other evidence in the case, in making its decision. These measures, which would not involve instructing a jury it may draw an adverse inference from loss of information, would be available under subdivision (e)(1) if no greater than necessary to cure prejudice. In addition, subdivision (e)(2) does not limit the discretion of courts to give traditional missing evidence instructions based on a party's failure to present evidence it has in its possession at the time of trial.

Subdivision (e)(2) requires a finding that the party acted with the intent to deprive another party of the information's use in the litigation. This finding may be made by the court when ruling on a pretrial motion, when presiding at a bench trial, or when deciding whether to give an adverse inference instruction at trial. If a court were to conclude that the intent finding should be made by a jury, the court's instruction should make clear that the jury may infer from the loss of the information that it was unfavorable to the party that lost it only if the jury first finds that the party acted with the intent to deprive another party of the information's use in the litigation. If the jury does not make this finding, it may not infer from the loss that the information was unfavorable to the party that lost it.

Subdivision (e)(2) does not include a requirement that the court find prejudice to the party deprived of the information. This is because the finding of intent required by the subdivision can support not only an inference that the lost information was unfavorable to the party that intentionally destroyed it, but also an inference that the opposing party was prejudiced by the loss of information that would have favored its position. Subdivision (e)(2) does not require any further finding of prejudice.

Courts should exercise caution, however, in using the measures specified in (e)(2). Finding an intent to deprive another party of the lost information's use in the litigation does not require a court to adopt any of the measures listed in subdivision (e)(2). The remedy should fit the wrong, and the severe measures authorized by this subdivision should not be used when the information lost was relatively unimportant or lesser measures such as those specified in subdivision (e)(1) would be sufficient to redress the loss.

Rule 45—Subpoena

- (a) In General.
 - (1) Form and Contents.
 - (A) Requirements—In General. Every subpoena must:
 - (i) state the court from which it issued;
 - (ii) state the title of the action and its civil-action number;
 - (iii) command each person to whom it is directed to do the following at a specified time and place: attend and testify; produce designated documents, electronically stored information, or tangible things in that person's possession, custody, or control; or permit the inspection of premises; and
 - (iv) set out the text of Rule 45(d) and (e).
 - (B) Command to Attend a Deposition—Notice of the Recording Method. A subpoena commanding attendance at a deposition must state the method for recording the testimony.
 - (C) Combining or Separating a Command to Produce or to Permit Inspection; Specifying the Form for Electronically Stored Information. A command to produce documents, electronically stored information, or tangible things or to permit the inspection of premises may be included in a subpoena commanding attendance at a deposition, hearing, or trial, or may be set out in a separate subpoena. A subpoena may specify the form or forms in which electronically stored information is to be produced.
 - (D) Command to Produce; Included Obligations. A command in a subpoena to produce documents, electronically stored information, or tangible things requires the responding person to permit inspection, copying, testing, or sampling of the materials.

- (2) Issuing Court. A subpoena must issue from the court where the action is pending.
- (3) Issued by Whom. The clerk must issue a subpoena, signed but otherwise in blank, to a party who requests it. That party must complete it before service. An attorney also may issue and sign a subpoena if the attorney is authorized to practice in the issuing court.
- (4) Notice to Other Parties Before Service. If the subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, then before it is served on the person to whom it is directed, a notice and a copy of the subpoena must be served on each party.
- (b) Service.
 - (1) By Whom and How; Tendering Fees. Any person who is at least 18 years old and not a party may serve a subpoena. Serving a subpoena requires delivering a copy to the named person and, if the subpoena requires that person's attendance, tendering the fees for 1 day's attendance and the mileage allowed by law. Fees and mileage need not be tendered when the subpoena issues on behalf of the United States or any of its officers or agencies.
 - (2) Service in the United States. A subpoena may be served at any place within the United States.
 - (3) Service in a Foreign Country. 28 U.S.C. § 1783 governs issuing and serving a subpoena directed to a United States national or resident who is in a foreign country.
 - (4) Proof of Service. Proving service, when necessary, requires filing with the issuing court a statement showing the date and manner of service and the names of the persons served. The statement must be certified by the server.
- (c) Place of Compliance.
 - (1) For a Trial, Hearing, or Deposition. A subpoena may command a person to attend a trial, hearing, or deposition only as follows:
 - (A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

- (B) within the state where the person resides, is employed, or regularly transacts business in person, if the person
 - (i) is a party or a party's officer; or
 - (ii) is commanded to attend a trial and would not incur substantial expense.
- (2) For Other Discovery. A subpoena may command:
 - (A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and
 - (B) inspection of premises at the premises to be inspected.
- (d) Protecting a Person Subject to a Subpoena; Enforcement.
 - (1) Avoiding Undue Burden or Expense; Sanctions. A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.
 - (2) Command to Produce Materials or Permit Inspection.
 - (A) Appearance Not Required. A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.
 - (B) Objections. A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

- (i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.
- (ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.
- (3) Quashing or Modifying a Subpoena.
 - (A) When Required. On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:
 - (i) fails to allow a reasonable time to comply;
 - (ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);
 - (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or
 - (iv) subjects a person to undue burden.
 - (B) When Permitted. To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:
 - (i) disclosing a trade secret or other confidential research, development, or commercial information; or
 - (ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.
 - (C) Specifying Conditions as an Alternative. In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:
 - (i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and
 - (ii) ensures that the subpoenaed person will be reasonably

compensated.

- (e) Duties in Responding to a Subpoena.
 - (1) Producing Documents or Electronically Stored Information. These procedures apply to producing documents or electronically stored information:
 - (A) Documents. A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.
 - (B) Form for Producing Electronically Stored Information Not Specified. If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.
 - (C) Electronically Stored Information Produced in Only One Form. The person responding need not produce the same electronically stored information in more than one form.
 - (D) Inaccessible Electronically Stored Information. The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.
 - (2) Claiming Privilege or Protection.
 - (A) Information Withheld. A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:
 - (i) expressly make the claim; and
 - (ii) describe the nature of the withheld documents, communications, or tangible things in a manner that,

without revealing information itself privileged or protected, will enable the parties to assess the claim.

- (B) Information Produced. If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.
- (f) *Transferring a Subpoena-Related Motion*. When the court where compliance is required did not issue the subpoena, it may transfer a motion under this rule to the issuing court if the person subject to the subpoena consents or if the court finds exceptional circumstances. Then, if the attorney for a person subject to a subpoena is authorized to practice in the court where the motion was made, the attorney may file papers and appear on the motion as an officer of the issuing court. To enforce its order, the issuing court may transfer the order to the court where the motion was made.
- (g) *Contempt*. The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

2006 Advisory Committee Notes

Rule 45 is amended to conform the provisions for subpoenas to changes in other discovery rules, largely related to discovery of electronically stored information. Rule 34 is amended to provide in greater detail for the production of electronically stored information. Rule 45(a)(1)(C) is amended to recognize that electronically stored information, as defined in Rule 34(a), can also be sought by subpoena. Like Rule 34(b), Rule 45(a)(1) is amended to provide that the subpoena can designate a form or forms for production of electronic data. Rule 45(c)(2) is amended, like Rule 34(b), to authorize the person served with a subpoena to object to the requested form or forms. In addition, as under Rule 34(b), Rule 45(d)(1)(B) is amended to provide that if the subpoena does not specify the form or forms for electronically stored information, the person served with the subpoena must produce electronically stored information in a form or forms in which it is usually maintained or in a form or forms that are reasonably usable. Rule 45(d)(1)(C) is added to provide that the person producing electronically stored information should not have to produce the same information in more than one form unless so ordered by the court for good cause.

As with discovery of electronically stored information from parties, complying with a subpoena for such information may impose burdens on the responding person. Rule 45(c) provides protection against undue impositions on nonparties. For example, Rule 45(c)(1) directs that a party serving a subpoena "shall take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena," and Rule 45(c)(2)(B) permits the person served with the subpoena to object to it and directs that an order requiring compliance "shall protect a person who is neither a party nor a party's officer from significant expense resulting from" compliance. Rule 45(d)(1)(D) is added to provide that the responding person need not provide discovery of electronically stored information from sources the party identifies as not reasonably accessible, unless the court orders such discovery for good cause, considering the limitations of Rule 26(b)(2)(C), on terms that protect a nonparty against significant expense. A parallel provision is added to Rule 26(b)(2).

Rule 45(a)(1)(B) is also amended, as is Rule 34(a), to provide that a subpoena is available to permit testing and sampling as well as inspection and copying. As in Rule 34, this change recognizes that on occasion the opportunity to perform testing or sampling may be important, both for documents and for electronically stored information. Because testing or sampling may present particular issues of burden or intrusion for the person served with the subpoena, however, the protective provisions of Rule 45(c) should be enforced with vigilance when such demands are made. Inspection or testing of certain types of electronically stored information or of a person's electronic information system may raise issues of confidentiality or privacy. The addition of sampling and testing to Rule 45(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a person's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.

Rule 45(d)(2) is amended, as is Rule 26(b)(5), to add a procedure for assertion of privilege or of protection as trial-preparation materials after production. The receiving party may submit the information to the court for resolution of the privilege claim, as under Rule 26(b)(5)(B).

Other minor amendments are made to conform the rule to the changes described above.

Changes Made After Publication and Comment. The Committee recommends a modified version of the proposal as published. The changes were made to maintain the parallels between Rule 45 and the other rules that address discovery of electronically stored information. These changes are fully described in the introduction to Rule 45 and in the discussions of the other rules.

Rule 53—Masters

- (a) Appointment.
 - (1) Scope. Unless a statute provides otherwise, a court may appoint a master only to:
 - (A) perform duties consented to by the parties;
 - (B) hold trial proceedings and make or recommend findings of fact on issues to be decided without a jury if appointment is warranted by:
 - (i) some exceptional condition; or
 - (ii) the need to perform an accounting or resolve a difficult computation of damages; or
 - (C) address pretrial and posttrial matters that cannot be effectively and timely addressed by an available district judge or magistrate judge of the district.
 - (2) Disqualification. A master must not have a relationship to the parties, attorneys, action, or court that would require disqualification of a judge under 28 U.S.C. § 455, unless the parties, with the court's approval, consent to the appointment after the master discloses any potential grounds for disqualification.
 - (3) Possible Expense or Delay. In appointing a master, the court must consider the fairness of imposing the likely expenses on the parties and must protect against unreasonable expense or delay.
- (b) Order Appointing a Master.
- (1) Notice. Before appointing a master, the court must give the parties notice and an opportunity to be heard. Any party may suggest candidates for appointment.
- (2) Contents. The appointing order must direct the master to proceed with all reasonable diligence and must state:
 - (A) the master's duties, including any investigation or enforcement duties, and any limits on the master's authority under Rule 53(c);
 - (B) the circumstances, if any, in which the master may communicate ex parte with the court or a party;
 - (C) the nature of the materials to be preserved and filed as the record of the master's activities;
 - (D) the time limits, method of filing the record, other procedures, and standards for reviewing the master's orders, findings, and recommendations; and
 - (E) the basis, terms, and procedure for fixing the master's compensation under Rule 53(g).
- (3) Issuing. The court may issue the order only after:
 - (A) the master files an affidavit disclosing whether there is any ground for disqualification under 28 U.S.C. § 455; and
 - (B) if a ground is disclosed, the parties, with the court's approval, waive the disqualification.
- (4) Amending. The order may be amended at any time after notice to the parties and an opportunity to be heard.
- (c) Master's Authority.
 - (1) In General. Unless the appointing order directs otherwise, a master may:
 - (A) regulate all proceedings;
 - (B) take all appropriate measures to perform the assigned duties fairly and efficiently; and
 - (C) if conducting an evidentiary hearing, exercise the appointing court's power to compel, take, and record evidence.

- (2) Sanctions. The master may by order impose on a party any noncontempt sanction provided by Rule 37 or 45, and may recommend a contempt sanction against a party and sanctions against a nonparty.
- (d) *Master's Orders*. A master who issues an order must file it and promptly serve a copy on each party. The clerk must enter the order on the docket.
- (e) *Master's Reports*. A master must report to the court as required by the appointing order. The master must file the report and promptly serve a copy on each party, unless the court orders otherwise.
- (f) Action on the Master's Order, Report, or Recommendations.
 - (1) Opportunity for a Hearing; Action in General. In acting on a master's order, report, or recommendations, the court must give the parties notice and an opportunity to be heard; may receive evidence; and may adopt or affirm, modify, wholly or partly reject or reverse, or resubmit to the master with instructions.
 - (2) Time to Object or Move to Adopt or Modify. A party may file objections to—or a motion to adopt or modify—the master's order, report, or recommendations no later than 21 days after a copy is served, unless the court sets a different time.
 - (3) Reviewing Factual Findings. The court must decide de novo all objections to findings of fact made or recommended by a master, unless the parties, with the court's approval, stipulate that:
 - (A) the findings will be reviewed for clear error; or
 - (B) the findings of a master appointed under Rule 53(a)(1)(A) or (C) will be final.
 - (4) Reviewing Legal Conclusions. The court must decide de novo all objections to conclusions of law made or recommended by a master.
 - (5) Reviewing Procedural Matters. Unless the appointing order establishes a different standard of review, the court may set aside a master's ruling on a procedural matter only for an abuse of discretion.
- (g) Compensation.

- (1) Fixing Compensation. Before or after judgment, the court must fix the master's compensation on the basis and terms stated in the appointing order, but the court may set a new basis and terms after giving notice and an opportunity to be heard.
- (2) Payment. The compensation must be paid either:
 - (A) by a party or parties; or
 - (B) from a fund or subject matter of the action within the court's cortrol.
- (3) Allocating Payment. The court must allocate payment among the parties after considering the nature and amount of the controversy, the parties' means, and the extent to which any party is more responsible than other parties for the reference to a master. An interim allocation may be amended to reflect a decision on the merits.
- (h) *Appointing a Magistrate Judge*. A magistrate judge is subject to this rule only when the order referring a matter to the magistrate judge states that the reference is made under this rule.

Rule 54—Judgment; Costs

- (a) *Definition; Form.* "Judgment" as used in these rules includes a decree and any order from which an appeal lies. A judgment should not include recitals of pleadings, a master's report, or a record of prior proceedings.
- (b) Judgment on Multiple Claims or Involving Multiple Parties. When an action presents more than one claim for relief—whether as a claim, counterclaim, crossclaim, or third-party claim—or when multiple parties are involved, the court may direct entry of a final judgment as to one or more, but fewer than all, claims or parties only if the court expressly determines that there is no just reason for delay. Otherwise, any order or other decision, however designated, that adjudicates fewer than all the claims or the rights and liabilities of fewer than all the parties does not end the action as to any of the claims or parties and may be revised at any time before the entry of a judgment adjudicating all the claims and all the parties' rights and liabilities.
- (c) *Demand for Judgment; Relief to Be Granted.* A default judgment must not differ in kind from, or exceed in amount, what is demanded in the pleadings

Every other final judgment should grant the relief to which each party is entitled, even if the party has not demanded that relief in its pleadings.

- (d) Costs; Attorney's Fees.
 - (1) Costs Other Than Attorney's Fees. Unless a federal statute, these rules, or a court order provides otherwise, costs—other than attorney's fees—should be allowed to the prevailing party. But costs against the United States, its officers, and its agencies may be imposed only to the extent allowed by law. The clerk may tax costs on 14 days' notice. On motion served within the next 7 days, the court may review the clerk's action.
 - (2) Attorney's Fees.
 - (A) Claim to Be by Motion. A claim for attorney's fees and related nontaxable expenses must be made by motion unless the substantive law requires those fees to be proved at trial as an element of damages.
 - (B) Timing and Contents of the Motion. Unless a statute or a court order provides otherwise, the motion must:
 - (i) be filed no later than 14 days after the entry of judgment;
 - (ii) specify the judgment and the statute, rule, or other grounds entitling the movant to the award;
 - (iii) state the amount sought or provide a fair estimate of it; and
 - (iv) disclose, if the court so orders, the terms of any agreement about fees for the services for which the claim is made.
 - (C) Proceedings. Subject to Rule 23(h), the court must, on a party's request, give an opportunity for adversary submissions on the motion in accordance with Rule 43(c) or 78. The court may decide issues of liability for fees before receiving submissions on the value of services. The court must find the facts and state its conclusions of law as provided in Rule 52(a).
 - (D) Special Procedures by Local Rule; Reference to a Master or a Magistrate Judge. By local rule, the court may establish special procedures to resolve fee-related issues without extensive evidentiary hearings. Also, the court may refer issues concerning the value of services to a special master under Rule 53 without

regard to the limitations of Rule 53(a)(1), and may refer a motion for attorney's fees to a magistrate judge under Rule 72(b) as if it were a dispositive pretrial matter.

(E) Exceptions. Subparagraphs (A)-(D) do not apply to claims for fees and expenses as sanctions for violating these rules or as sanctions under 28 U.S.C. § 1927.



Appendix C

Select Texas Rules of Civil Procedure

Rule 1 Objective of Rules

Effective September 1, 1941

The proper objective of rules of civil procedure is to obtain a just, fair, equitable and impartial adjudication of the rights of litigants under established principles of substantive law. To the end that this objective may be attained with as great expedition and dispatch and at the least expense both to the litigants and to the state as may be practicable, these rules shall be given liberal construction.

Rule 171 Master in Chancery

Effective December 31, 1941

The court may, in exceptional cases, for good cause appoint a master in chancery, who shall be a citizen of this State, and not an attorney for either party to the action, nor related to either party, who shall perform all of the duties required of him by the court, and shall be under orders of the court, and have such power as the master of chancery has in a court of equity.

The order of reference to the master may specify or limit his powers, and may direct him to report only upon particular issues, or to do or perform particular acts, or to receive and report evidence only and may fix the time and place for beginning and closing the hearings, and for the filing of the master's report. Subject to the limitations and specifications stated in the order, the master has and shall exercise the power to regulate all proceedings in every hearing before him and to do all acts and take all measures necessary or proper for the efficient performance of his duties under the order. He may require the production before him of evidence upon all matters embraced in the reference, including the production of books, papers, vouchers, documents and other writings applicable thereto. He may rule upon the admissibility of evidence, unless otherwise directed by the order of reference and has the authority to put witnesses on oath, and may, himself, examine them, and may call the parties to the action and examine them upon oath. When a party so requests, the master shall make a record of the evidence offered and excluded in the same manner as provided for a court sitting in the trial of a case.

Appendix C

The clerk of the court shall forthwith furnish the master with a copy of the order of reference.

The parties may procure the attendance of witnesses before the master by the issuance and service of process as provided by law and these rules.

The court may confirm, modify, correct, reject, reverse or recommit the report, after it is filed, as the court may deem proper and necessary in the particular circumstances of the case. The court shall award reasonable compensation to such master to be taxed as costs of suit.

Rule 176.6 Subpoenas—Response

Effective January 1, 1999

- (a) Compliance Required. Except as provided in this subdivision, a person served with a subpoena must comply with the command stated therein unless discharged by the court or by the party summoning such witness. A person commanded to appear and give testimony must remain at the place of deposition, hearing, or trial from day to day until discharged by the court or by the party summoning the witness.
- (b) Organizations. If a subpoena commanding testimony is directed to a corporation, partnership, association, governmental agency, or other organization, and the matters on which examination is requested are described with reasonable particularity, the organization must designate one or more persons to testify on its behalf as to matters known or reasonably available to the organization.
- (c) Production of Documents or Tangible Things. A person commanded to produce documents or tangible things need not appear in person at the time and place of production unless the person is also commanded to attend and give testimony, either in the same subpoena or a separate one. A person must produce documents as they are kept in the usual course of business or must organize and label them to correspond with the categories in the demand. A person may withhold material or information claimed to be privileged but must comply with Rule 193.3. A nonparty's production of a document authenticates the document for use against the nonparty to the same extent as a party's production of a document is authenticated for use against the party under Rule 193.7.

- (d) Objections. A person commanded to produce or permit inspection or copying of designated documents and things may serve on the party requesting issuance of the subpoena—before the time specified for compliance—written objections to producing any or all of the designated materials. A person need not comply with the part of a subpoena to which objection is made as provided in this paragraph unless ordered to do so by the court. The party requesting the subpoena may move for such an order at any time after an objection is made.
- (e) Protective Orders. A person commanded to appear at a deposition, hearing, or trial, or to produce and permit inspection and copying of designated documents and things, and any other person affected by the subpoena, may move for a protective order under Rule 192.6(b)—before the time specified for compliance—either in the court in which the action is pending or in a district court in the county where the subpoena was served. The person must serve the motion on all parties in accordance with Rule 21a. A person need not comply with the part of a subpoena from which protection is sought under this paragraph unless ordered to do so by the court. The party requesting the subpoena may seek such an order at any time after the motion for protection is filed.
- (f) *Trial Subpoenas*. A person commanded to attend and give testimony, or to produce documents or things, at a hearing or trial, may object or move for protective order before the court at the time and place specified for compliance, rather than under paragraphs (d) and (e).

Rule 176.7 Subpoenas—Protection of Person from Undue Burden and Expense

Effective January 1, 1999

A party causing a subpoena to issue must take reasonable steps to avoid imposing undue burden or expense on the person served. In ruling on objections or motions for protection, the court must provide a person served with a subpoena an adequate time for compliance, protection from disclosure of privileged material or information, and protection from undue burden or expense. The court may impose reasonable conditions on compliance with a subpoena, including compensating the witness for undue hardship.

Rule 191.2 Conference

Effective January 1, 1999

Parties and their attorneys are expected to cooperate in discovery and to make any agreements reasonably necessary for the efficient disposition of the case. All discovery motions or requests for hearings relating to discovery must contain a certificate by the party filing the motion or request that a reasonable effort has been made to resolve the dispute without the necessity of court intervention and the effort failed.

Rule 191.3 Signing of Disclosures, Discovery Requests, Notices, Responses, and Objections

Effective January 1, 1999

- (a) *Signature Required*. Every disclosure, discovery request, notice, response, and objection must be signed:
 - (1) by an attorney, if the party is represented by an attorney, and must show the attorney's State Bar of Texas identification number, address, telephone number, and fax number, if any; or
 - (2) by the party, if the party is not represented by an attorney, and must show the party's address, telephone number, and fax number, if any.
- (b) Effect of Signature on Disclosure. The signature of an attorney or party on a disclosure constitutes a certification that to the best of the signer's knowledge, information, and belief, formed after a reasonable inquiry, the disclosure is complete and correct as of the time it is made.
- (c) Effect of Signature on Discovery Request, Notice, Response, or Objection. The signature of an attorney or party on a discovery request, notice, response, or objection constitutes a certification that to the best of the signer's knowledge, information, and belief, formed after a reasonable inquiry, the request, notice, response, or objection:
 - is consistent with the rules of civil procedure and these discovery rules and warranted by existing law or a good faith argument for the extension, modification, or reversal of existing law;
 - (2) has a good faith factual basis;

- (3) is not interposed for any improper purpose, such as to harass or to cause unnecessary delay or needless increase in the cost of litigation; and
- (4) is not unreasonable or unduly burdensome or expensive, given the needs of the case, the discovery already had in the case, the amount in controversy, and the importance of the issues at stake in the litigation.
- (d) Effect of Failure to Sign. If a request, notice, response, or objection is not signed, it must be stricken unless it is signed promptly after the omission is called to the attention of the party making the request, notice, response, or objection. A party is not required to take any action with respect to a request or notice that is not signed.
- (e) Sanctions. If the certification is false without substantial justification, the court may, upon motion or its own initiative, impose on the person who made the certification, or the party on whose behalf the request, notice, response, or objection was made, or both, an appropriate sanction as for a frivolous pleading or motion under Chapter 10 of the Civil Practice and Remedies Code.

Rule 192.4 Limitations on Scope of Discovery

Effective January 1, 1999

The discovery methods permitted by these rules should be limited by the court if it determines, on motion or on its own initiative and on reasonable notice, that:

- (a) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; or
- (b) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.

Rule 192.6 Protective Orders

Effective January 1, 1999

- (a) Motion. A person from whom discovery is sought, and any other person affected by the discovery request, may move within the time permitted for response to the discovery request for an order protecting that person from the discovery sought. A person should not move for protection when an objection to written discovery or an assertion of privilege is appropriate, but a motion does not waive the objection or assertion of privilege. If a person seeks protection regarding the time or place of discovery, the person must state a reasonable time and place for discovery with which the person will comply. A person must comply with a request to the extent protection is not sought unless it is unreasonable under the circumstances to do so before obtaining a ruling on the motion.
- (b) Order. To protect the movant from undue burden, unnecessary expense, harassment, annoyance, or invasion of personal, constitutional, or property rights, the court may make any order in the interest of justice and may among other things—order that:
 - (1) the requested discovery not be sought in whole or in part;
 - (2) the extent or subject matter of discovery be limited;
 - (3) the discovery not be undertaken at the time or place specified;
 - (4) the discovery be undertaken only by such method or upon such terms and conditions or at the time and place directed by the court;
 - (5) the results of discovery be sealed or otherwise protected, subject to the provisions of Rule 76a.

Notes and Comments

Comment to 1999 change:

 While the scope of discovery is quite broad, it is nevertheless confined by the subject matter of the case and reasonable expectations of obtaining information that will aid resolution of the dispute. The rule must be read and applied in that context. See In re American Optical Corp., _S.W.2d_ (Tex. 1998) (per curiam); K-Mart v. Sanderson, 937 S.W.2d 429 (Tex. 1996) (per curiam); Dillard Dept. Stores v. Hall, 909 S.W.2d 491 (Tex. 1995) (per curiam); Texaco, Inc. v. Sanderson, 898 S.W.2d 813 (Tex. 1995) (per curiam); Loftin v. Martin, 776 S.W.2d 145, 148 (Tex. 1989).

- 2. The definition of documents and tangible things has been revised to clarify that things relevant to the subject matter of the action are within the scope of discovery regardless of their form.
- 3. Rule 192.3(c) makes discoverable a "brief statement of each identified person's connection with the case." This provision does not contemplate a narrative statement of the facts the person knows, but at most a few words describing the person's identity as relevant to the lawsuit. For instance: "treating physician," "eyewitness," "chief financial officer," "director," "plaintiff's mother and eyewitness to accident." The rule is intended to be consistent with Axelson v. McIlhany, 798 S.W.2d 550 (Tex. 1990).
- 4. Rule 192.3(g) does not suggest that settlement agreements in other cases are relevant or irrelevant.
- 5. Rule 192.3(j) makes a party's legal and factual contentions discoverable but does not require more than a basic statement of those contentions and does not require a marshaling of evidence.
- 6. The sections in former Rule 166b concerning land and medical records are not included in this rule. They remain within the scope of discovery and are discussed in other rules.
- 7. The court's power to limit discovery based on the needs and circumstances of the case is expressly stated in Rule 192.4. The provision is taken from Rule 26(b)(2) of the Federal Rules of Civil Procedure. Courts should limit discovery under this rule only to prevent unwarranted delay and expense as stated more fully in the rule. A court abuses its discretion in unreasonably restricting a party's access to information through discovery.
- 8. Work product is defined for the first time, and its exceptions stated. Work product replaces the "attorney work product" and "party communication" discovery exemptions from former Rule 166b.
- 9. Elimination of the "witness statement" exemption does not render all witness statements automatically discoverable but subjects them to the same rules concerning the scope of discovery and privileges applicable to other documents or tangible things.

Rule 193.1 Responding to Written Discovery; Duty to Make Complete Response

Effective January 1, 1999

A party must respond to written discovery in writing within the time provided by court order or these rules. When responding to written discovery, a party must make a complete response, based on all information reasonably available to the responding party or its attorney at the time the response is made. The responding party's answers, objections, and other responses must be preceded by the request to which they apply.

Rule 193.2 Objecting to Written Discovery

Effective January 1, 1999

- (a) Form and Time for Objections. A party must make any objection to written discovery in writing—either in the response or in a separate documentwithin the time for response. The party must state specifically the legal or factual basis for the objection and the extent to which the party is refusing to comply with the request.
- (b) Duty to Respond When Partially Objecting; Objection to Time or Place of Production. A party must comply with as much of the request to which the party has made no objection unless it is unreasonable under the circumstances to do so before obtaining a ruling on the objection. If the responding party objects to the requested time or place of production, the responding party must state a reasonable time and place for complying with the request and must comply at that time and place without further request or order.
- (c) *Good Faith Basis for Objection.* A party may object to written discovery only if a good faith factual and legal basis for the objection exists at the time the objection is made.
- (d) Amendment. An objection or response to written discovery may be amended or supplemented to state an objection or basis that, at the time the objection or response initially was made, either was inapplicable or was unknown after reasonable inquiry.
- (e) *Waiver of Objection.* An objection that is not made within the time required, or that is obscured by numerous unfounded objections, is waived unless the court excuses the waiver for good cause shown.
- (f) No Objection to Preserve Privilege. A party should not object to a request for written discovery on the grounds that it calls for production of material

or information that is privileged but should instead comply with Rule 193.3. A party who objects to production of privileged material or information does not waive the privilege but must comply with Rule 193.3 when the error is pointed out.

Rule 193.3 Asserting a Privilege

Effective January 1, 1999

A party may preserve a privilege from written discovery in accordance with this subdivision.

- (a) *Withholding Privileged Material or Information*. A party who claims that material or information responsive to written discovery is privileged may withhold the privileged material or information from the response. The party must state—in the response (or an amended or supplemental response) or in a separate document—that:
 - (1) information or material responsive to the request has been withheld,
 - (2) the request to which the information or material relates, and
 - (3) the privilege or privileges asserted.
- (b) Description of Withheld Material or Information. After receiving a response indicating that material or information has been withheld from production, the party seeking discovery may serve a written request that the withholding party identify the information and material withheld. Within 15 days of service of that request, the withholding party must serve a response that:
 - describes the information or materials withheld that, without revealing the privilegec information itself or otherwise waiving the privilege, enables other parties to assess the applicability of the privilege, and
 - (2) asserts a specific privilege for each item or group of items withheld.
- (c) *Exemption.* Without complying with paragraphs (a) and (b), a party may withhold a privileged communication to or from a lawyer or lawyer's representative or a privileged document of a lawyer or lawyer's representative—

- created or made from the point at which a party consults a lawyer with a view to obtaining professional legal services from the lawyer in the prosecution or defense of a specific claim in the litigation in which discovery is requested, and
- (2) concerning the litigation in which the discovery is requested.
- (d) Privilege Not Waived by Production. A party who produces material or information without intending to waive a claim of privilege does not waive that claim under these rules or the Rules of Evidence if—within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made—the producing party amends the response, identifying the material or information produced and stating the privilege asserted. If the producing party thus amends the response to assert a privilege, the requesting party must promptly return the specified material or information and any copies pending any ruling by the court denying the privilege.

Rule 193.4 Hearing and Ruling on Objections and Assertions of Privilege

Effective January 1, 1999

- (a) Hearing. Any party may at any reasonable time request a hearing on an objection or claim of privilege asserted under this rule. The party making the objection or asserting the privilege must present any evidence necessary to support the objection or privilege. The evidence may be testimony presented at the hearing or affidavits served at least seven days before the hearing or at such other reasonable time as the court permits. If the court determines that an in camera review of some or all of the requested discovery is necessary, that material or information must be segregated and produced to the court in a sealed wrapper within a reasonable time following the hearing.
- (b) Ruling. To the extent the court sustains the objection or claim of privilege, the responding party has no further duty to respond to that request. To the extent the court overrules the objection or claim of privilege, the responding party must produce the requested material or information within 30 days after the court's ruling or at such time as the court orders. A party need not request a ruling on that party's own objection or assertion of privilege to preserve the objection or privilege.

(c) Use of Material or Information Withheld Under Claim of Privilege. A party may not use—at any hearing or trial—material or information withheld from discovery under a claim of privilege, including a claim sustained by the court, without timely amending or supplementing the party's response to that discovery.

Rule 193.5 Amending or Supplementing Responses to Written Discovery

Effective January 1, 1999

- (a) *Duty to Amend or Supplement*. If a party learns that the party's response to written discovery was incomplete or incorrect when made, or, although complete and correct when made, is no longer complete and correct, the party must amend or supplement the response:
 - (1) to the extent that the written discovery sought the identification of persons with knowledge of relevant facts, trial witnesses, or expert witnesses, and
 - (2) the extent that the written discovery sought other information, unless the additional or corrective information has been made known to the other parties in writing, on the record at a deposition, or through other discovery responses.
- (b) Time and Form of Amended or Supplemental Response. An amended or supplemental response must be made reasonably promptly after the party discovers the necessity for such a response. Except as otherwise provided by these rules, it is presumed that an amended or supplemental response made less than 30 days before trial was not made reasonably promptly. An amended or supplemental response must be in the same form as the initial response and must be verified by the party if the original response was required to be verified by the party, but the failure to comply with this requirement does not make the amended or supplemental response untimely unless the party making the response refuses to correct the defect within a reasonable time after it is pointed out.

Rule 193.6 Failing to Timely Respond—Effect on Trial

Effective January 1, 1999

(a) *Exclusion of Evidence and Exceptions*. A party who fails to make, amend, or supplement a discovery response in a timely manner may not introduce in

evidence the material or information that was not timely disclosed, or offer the testimony of a witness (other than a named party) who was not timely identified, unless the court finds that:

- (1) there was good cause for the failure to timely make, amend, or supplement the discovery response; or
- (2) the failure to timely make, amend, or supplement the discovery response will not unfairly surprise or unfairly prejudice the other parties.
- (b) *Burden of Establishing Exception.* The burden of establishing good cause or the lack of unfair surprise or unfair prejudice is on the party seeking to introduce the evidence or call the witness. A finding of good cause or of the lack of unfair surprise or unfair prejudice must be supported by the record.
- (c) Continuance. Even if the party seeking to introduce the evidence or call the witness fails to carry the burden under paragraph (b), the court may grant a continuance or temporarily postpone the trial to allow a response to be made, amended, or supplemented, and to allow opposing parties to conduct discovery regarding any new information presented by that response.

Rule 193.7 Production of Documents Self-Authenticating

Effective January 1, 1999

A party's production of a document in response to written discovery authenticates the document for use against that party in any pretrial proceeding or at trial unless within ten days or a longer or shorter time ordered by the court, after the producing party has actual notice that the document will be used—the party objects to the authenticity of the document, or any part of it, stating the specific basis for objection. An objection must be either on the record or in writing and must have a good faith factual and legal basis. An objection made to the authenticity of only part of a document does not affect the authenticity of the remainder. If objection is made, the party attempting to use the document should be given a reasonable opportunity to establish its authenticity.

Notes and Comments

Comment to 1999 change:

- 1. This rule imposes a duty upon parties to make a complete response to written discovery based upon all information reasonable available, subject to objections and privileges.
- 2. An objection to a written discovery does not excuse the responding party from complying with the request to the extent no objection is made. But a party may object to a request for "all documents relevant to the lawsuit" as overly broad and not in compliance with the rule requiring specific requests for documents and refuse to comply with it entirely. See Loftin v. Martin, 776 S.W.2d 145 (Tex. 1989). A party may also object to a request for a litigation file on the ground that it is overly broad and may assert that on its face the request seeks only materials protected by privilege. See National Union Fire Ins. Co. v. Valdez, 863 S.W.2d 458 (Tex. 1993). A party who objects to production of documents from a remote time period should produce documents from a more recent period unless that production would be burdensome and duplicative should the objection be overruled.
- This rule governs the presentation of all privileges including work product. It 3. dispenses with objections to written discovery requests on the basis that responsive information or materials are protected by a specific privilege from discovery. Instead, the rule requires parties to state that information or materials have been withheld and to identify the privilege upon which the party relies. The statement should not be made prophylactically, but only when specific information and materials have been withheld. The party must amend or supplement the statement if additional privileged information or material is found subsequent to the initial response. Thus, when large numbers of documents are being produced, a party may amend the initial response when documents are found as to which the party claims privilege. A party need not state that material created by or for lawyers for the litigation has been withheld as it can be assumed that such material will be withheld from virtually any request on the grounds of attorney-client privilege or work product. However, the rule does not prohibit a party from specifically requesting the material or information if the party has a good faith basis for asserting that it is discoverable. An example would be material or informaticn described by Rule 503(d)(1) of the Rules of Evidence.
- 4. Rule 193.3(d) is a new provision that allows a party to assert a claim of privilege to material or information produced inadvertently without intending to waive the privilege. The provision is commonly used in complex cases to reduce costs and risks in large document productions. The focus is on the intent to waive the privilege, not the intent to produce the material or information. A

party who fails to diligently screen documents before producing them does not waive a claim of privilege. This rule is thus broader than Tex. R. Evid. 511 and overturns Granada Corp. v. First Court of Appeals, 844 S.W.2d 223 (Tex. 1992), to the extent the two conflict. The ten-day period (which may be short-ened by the court) allowed for an amended response does not run from the production of the material or information but from the party's first awareness of the mistake. To avoid complications at trial, a party may identify prior to trial the documents intended to be offered, thereby triggering the obligation to assert any overlooked privilege under this rule. A trial court may also order this procedure.

- 5. This rule imposes no duty to supplement or amend deposition testimony. The only duty to supplement deposition testimony is provided in Rule 195.6.
- 6. Any party can request a hearing in which the court will resolve issues brought up in objections or withholding statements. The party seeking to avoid discovery has the burden of proving the objection or privilege.
- 7. The self-authenticating provision is new. Authentication is, of course, but a condition precedent to admissibility and does not establish admissibility. See Tex. R. Evid. 901(a). The ten-day period allowed for objection to authenticity (which period may be altered by the court in appropriate circumstances) does not run from the production of the material or information but from the party's actual awareness that the document will be used. To avoid complications at trial, a party may identify prior to trial the documents intended to be offered, thereby triggering the obligation to object to authenticity. A trial court may also order this procedure. An objection to authenticity must be made in good faith.

Rule 196.1 Request for Production and Inspection to Parties Effective January 1, 1999

- (a) Request. A party may serve on another party—no later than 30 days before the end of the discovery period—a request for production or for inspection, to inspect, sample, test, photograph and copy documents or tangible things within the scope of discovery.
- (b) Contents of Request. The request must specify the items to be produced or inspected, either by individual item or by category, and describe with reasonable particularity each item and category. The request must specify a reasonable time (on or after the date on which the response is due) and place for production. If the requesting party will sample or test the requested

items, the means, manner and procedure for testing or sampling must be described with sufficient specificity to inform the producing party of the means, manner, and procedure for testing or sampling.

- (c) Requests for Production of Medical or Mental Health Records Regarding Nonparties.
 - (1) Service of Request on Nonparty. If a party requests another party to produce medical or mental health records regarding a nonparty, the requesting party must serve the nonparty with the request for production under Rule 21a.
 - (2) Exceptions. A party is not required to serve the request for production on a nonparty whose medical records are sought if:
 - (A) the nonparty signs a release of the records that is effective as to the requesting party;
 - (B) the identity of the nonparty whose records are sought will not directly or indirectly be disclosed by production of the records; or
 - (C) the court, upon a showing of good cause by the party seeking the records, orders that service is not required.
 - (3) *Confidentiality.* Nothing in this rule excuses compliance with laws concerning the confidentiality of medical or mental health records.

Rule 196.2 Response to Request for Production and Inspection Effective January 1, 1999

- (a) *Time for Response.* The responding party must serve a written response on the requesting party within 30 days after service of the request, except that a defendant served with a request before the defendant's answer is due need not respond until 50 days after service of the request.
- (b) *Content of Response.* With respect to each item or category of items, the responding party must state objections and assert privileges as required by these rules, and state, as appropriate, that:
 - (1) production, inspection, or other requested action will be permitted as requested;

- (2) the requested items are being served on the requesting party with the response;
- (3) production, inspection, or other requested action will take place at a specified time and place, if the responding party is objecting to the time and place of production; or
- (4) no items have been identified—after a diligent search—that are responsive to the request.

Rule 196.3 Production

Effective January 1, 1999

- (a) Time and Place of Production. Subject to any objections stated in the response, the responding party must produce the requested documents or tangible things within the person's possession, custody or control at either the time and place requested or the time and place stated in the response, unless otherwise agreed by the parties or ordered by the court, and must provide the requesting party a reasonable opportunity to inspect them.
- (b) Copies. The responding party may produce copies in lieu of originals unless a question is raised as to the authenticity of the original or in the circumstances it would be unfair to produce copies in lieu of originals. If originals are produced, the responding party is entitled to retain the originals while the requesting party inspects and copies them.
- (c) *Organization.* The responding party must either produce documents and tangible things as they are kept in the usual course of business or organize and label them to correspond with the categories in the request.

Rule 196.4 Electronic or Magnetic Data

Effective January 1, 1999

To obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced. The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If the responding party cannot—through reasonable efforts—retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules. If the court orders the responding party to comply with the request, the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.

Rule 196.5 Destruction or Alteration

Effective January 1, 1999

Testing, sampling or examination of an item may not destroy or materially alter an item unless previously authorized by the court.

Rule 196.6 Expenses of Production

Effective January 1, 1999

Unless otherwise ordered by the court for good cause, the expense of producing items will be borne by the responding party and the expense of inspecting, sampling, testing, photographing, and copying items produced will be borne by the requesting party.

Notes and Comments

Comment to 1999 change:

- 1. "Document and tangible things" are defined in Rule 192.3(b).
- 2. A party requesting sampling or testing must describe the procedure with sufficient specificity to enable the responding party to make any appropriate objections.
- 3. A party requesting production of magnetic or electronic data must specifically request the data, specify the form in which it wants the data produced, and specify any extraordinary steps for retrieval and translation. Unless ordered otherwise, the responding party need only produce the data reasonably available in the ordinary course of business in reasonably usable form.
- 4. The rule clarifies how the expenses of production are to be allocated absent a court order to the contrary.
- 5. The obligation of parties to produce documents within their possession, custody or control is explained in Rule 192.3(b).
- 6. Parties may request production and inspection of documents and tangible things from nonparties under Rule 205.3.

Appendix C

7. Rule 196.3(b) is based on Tex. R. Evid. 1003.8. Rule 196.1(c) is merely a notice requirement and does not expand the scope of discovery of a nonparty's medical records.

Rule 205.1 Discovery from Nonparties—Forms of Discovery; Subpoena Requirement

Effective January 1, 1999

A party may compel discovery from a nonparty—that is, a person who is not a party or subject to a party's control—only by obtaining a court order under Rules 196.7, 202, or 204, or by serving a subpoena compelling:

- (a) an oral deposition;
- (b) a deposition on written questions;
- (c) a request for production of documents or tangible things, pursuant to Rule 199.2(b)(5) or Rule 200.1(b), served with a notice of deposition on oral examination or written questions; and
- (d) a request for production of documents and tangible things under this rule.

Rule 205.2 Discovery from Nonparties—Notice

Effective January 1, 1999

A party seeking discovery by subpoena from a nonparty must serve, on the nonparty and all parties, a copy of the form of notice required under the rules governing the applicable form of discovery. A notice of oral or written deposition must be served before or at the same time that a subpoena compelling attendance or production under the notice is served. A notice to produce documents or tangible things under Rule 205.3 must be served at least 10 days before the subpoena compelling production is served.

Rule 205.3 Discovery from Nonparties—Production of Documents and Tangible Things Without Deposition

Effective January 1, 1999

(a) *Notice; Subpoena.* A party may compel production of documents and tangible things from a nonparty by serving—a reasonable time before the response is due but no later than 30 days before the end of any applicable discovery period—the notice required in Rule 205.2 and a subpoena compelling production or inspection of documents or tangible things.

- (b) Contents of Notice. The notice must state:
 - (1) the name of the person from whom production or inspection is sought to be compelled;
 - (2) a reasonable time and place for the production or inspection; and
 - (3) the items to be produced or inspected, either by individual item or by category, describing each item and category with reasonable particularity, and, if applicable, describing the desired testing and sampling with sufficient specificity to inform the nonparty of the means, manner, and procedure for testing or sampling.
- (c) Requests for Production of Medical or Mental Health Records of Other Nonparties. If a party requests a nonparty to produce medical or mental health records of another non-party, the requesting party must serve the nonparty whose records are sought with the notice required under this rule. This requirement does not apply under the circumstances set forth in Rule 196.1(c)(2).
- (d) *Response.* The nonparty must respond to the notice and subpoena in accordance with Rule 176.6.
- (e) *Custody, Inspection and Copying.* The party obtaining the production must make all materials produced available for inspection by any other party on reasonable notice, and must furnish copies to any party who requests at that party's expense.
- (f) *Cost of Production*. A party requiring production of documents by a nonparty must reimburse the nonparty's reasonable costs of production.

Rule 215.2 Failure to Comply with Order or with Discovery Request Effective January 1, 1999

(a) Sanctions by Court in District Where Deposition is Taken. If a deponent fails to appear or to be sworn or to answer a question after being directed to do so by a district court in the district in which the deposition is being taken, the failure may be considered a contempt of that court.

- (b) Sanctions by Court in Which Action is Pending. If a party or an officer, director, or managing agent of a party or a person designated under Rules 199.2(b)(1) or 200.1(b) to testify on behalf of a party fails to comply with proper discovery requests or to obey an order to provide or permit discovery, including an order made under Rules 204 or 215.1, the court in which the action is pending may, after notice and hearing, make such orders in regard to the failure as are just, and among others the following:
 - an order disallowing any further discovery of any kind or of a particular kind by the disobedient party;
 - (2) an order charging all or any portion of the expenses of discovery or taxable court costs or both against the disobedient party or the attorney advising him;
 - (3) an order that the matters regarding which the order was made or any other designated facts shall be taken to be established for the purposes of the action in accordance with the claim of the party obtaining the order;
 - (4) an order refusing to allow the disobedient party to support or oppose designated claims or defenses, or prohibiting him from introducing designated matters in evidence;
 - (5) an order striking out pleadings or parts thereof, or staying further proceedings until the order is obeyed, or dismissing with or without prejudice the action or proceedings or any part thereof, or rendering a judgment by default against the disobedient party;
 - (6) in lieu of any of the foregoing orders or in addition thereto, an order treating as a contempt of court the failure to obey any orders except an order to submit to a physical or mental examination;
 - (7) when a party has failed to comply with an order under Rule 204 requiring him to appear or produce another for examination, such orders as are listed in paragraphs (1), (2), (3), (4) or (5) of this subdivision, unless the person failing to comply shows that he is unable to appear or to produce such person for examination.
 - (8) In lieu of any of the foregoing orders or in addition thereto, the court shall require the party failing to obey the order or the attorney advising him, or both, to pay, at such time as ordered by the court, the reasonable expenses, including attorney fees, caused

by the failure, unless the court finds that the failure was substantially justified or that other circumstances make an award of expenses unjust. Such an order shall be subject to review on appeal from the final judgment.

(c) Sanctions Against Nonparty For Violation of Rules 196.7 or 205.3. If a nonparty fails to comply with an order under Rules 196.7 or 205.3, the court which made the order may treat the failure to obey as contempt of court.

Rule 215.3 Abuse of Discovery Process in Seeking, Making, or Resisting Discovery

Effective January 1, 1999

If the court finds a party is abusing the discovery process in seeking, making or resisting discovery or if the court finds that any interrogatory or request for inspection or production is unreasonably frivolous, oppressive, or harassing, or that a response or answer is unreasonably frivolous or made for purposes of delay, then the court in which the action is pending may, after notice and hearing, impose any appropriate sanction authorized by paragraphs (1), (2), (3), (4), (5), and (8) of Rule 215.2(b). Such order of sanction shall be subject to review on appeal from the final judgment.



Appendix D

Updates to Texas Rules of Civil Procedure

Effective January 1, 2021

Essentials of E-Discovery

IN THE SUPREME COURT OF TEXAS

Misc. Docket No. 20-9101

ORDER AMENDING TEXAS RULES OF CIVIL PROCEDURE 47, 169, 190, 192, 193, 194, AND 195

ORDERED that:

- 1. In accordance with the Act of May 27, 2019, 86th Leg., R.S., ch. 696 (SB 2342), the Supreme Court approves the following amendments to Rules 47, 169, 190, 192, 193, 194, and 195 of the Texas Rules of Civil Procedure.
- 2. The amendments take effect January 1, 2021, and apply to cases filed on or after January 1, 2021, except for those filed in justice court.
- 3. The amendments may be changed before January 1, 2021, in response to public comments. Written comments should be sent to <u>rulescomments@txcourts.gov</u>. The Court requests that comments be sent by December 1, 2020.
- 4. Because the Court previously approved amendments to Rule 47, effective September 1, 2020 (Misc. Dkt. No. 20-9070), the amendments to Rule 47 approved in this Order are shown in redline against the version of Rule 47 that takes effect September 1, 2020.
- 5. The Clerk is directed to:
 - a. file a copy of this Order with the Secretary of State;
 - b. cause a copy of this Order to be mailed to each registered member of the State Bar of Texas by publication in the *Texas Bar Journal*;
 - c. send a copy of this Order to each elected member of the Legislature; and
 - d. submit a copy of the Order for publication in the Texas Register.

Dated: August 21, 2020

Nathan L. Hecht, Chief Justice

a aum Paul W. Green, Justice

Guzman. Justice

Debra H ehrmann. Justice

John P Dev Justice le,

James D. Blacklock, Justice

to a Busby, Justice

Jan Bland, Justice

Misc. Docket 20-9101

RULE 47. CLAIMS FOR RELIEF

An original pleading which sets for a claim for relief, whether an original petition, counterclaim, cross-claim, or third party claim, shall contain:

- (a) a short statement of the cause of action sufficient to give fair notice of the claim involved;
- (b) a statement that the damages sought are within the jurisdictional limits of the court;
- (c) except in suits governed by the Family Code, a statement that the party seeks:
 - only monetary relief of \$100,000250,000 or less, including damages of any kind, penalties, costs, expenses, pre-judgment interest, and attorney feesexcluding interest, statutory or punitive damages and penalties, and attorney's fees and costs; or
 - (2) monetary relief of \$100,000250,000 or less and non-monetary relief; or
 - (3) monetary relief over \$100,000 but not more than \$250,000; or
 - (43) monetary relief over \$250,000 but not more than \$1,000,000; or
 - (54) monetary relief over \$1,000,000; and

(d) a demand for judgment for all the other relief to which the party deems himself entitled.

Relief in the alternative or of several different types may be demanded; provided, further, that upon special exception the court shall require the pleader to amend so as to specify the maximum amount claimed. A party that fails to comply with (c) may not conduct discovery until the party's pleading is amended to comply.

Comment to 2021 change: Rule 47 is amended to implement section 22.004(h-1) of the Texas Government Code. A suit in which the original petition contains the statement in paragraph (c)(1) is governed by the expedited actions process in Rule 169.

RULE 169. EXPEDITED ACTIONS

- (a) Application.
 - (1) The expedited actions process in this rule applies to suit in which all claimants, other than counter-claimants, affirmatively plead that they seek only monetary relief aggregating \$100,000250,000 or less, including damages of any kind, penalties, costs, expenses, pre-judgment interest, and attorney feesexcluding interest, statutory or punitive damages and penalties, and attorney's fees and costs.

Misc. Docket 20-9101

- (2) The expedited actions process does not apply to a suit in which a party has filed a claim governed by the Family Code, the Property Code, the Tax Code, or Chapter 74 of the Civil Practice & Remedies Code.
- (b) Recovery. In no event may a party who prosecutes a suit under this rule recover a judgment in excess of \$100,000250,000, excluding post judgment interest, statutory or punitive damages and penalties, and attorney's fees and costs.
- (c) Removal from Process.
 - (1) A court must remove a suit from the expedited actions process:
 - (A) on motion and a showing of good cause by any party; or
 - (B) if any claimant, other than a counter-claimant, files a pleading or an amended or supplemental pleading that seeks any relief other than the monetary relief allowed by (a)(1).
 - (2) A pleading, amended pleading, or supplemental pleading that removes a suit from the expedited actions process may not be filed without leave of court unless it is filed before the earlier of 30 days after the discovery period is closed or 30 days before the date set for trial. Leave to amend may be granted only if good cause for filing the pleading outweighs any prejudice to an opposing party.
 - (3) If a suit is removed from the expedited actions process, the court must reopen discovery under Rule 190.2(c).
- (d) Expedited Actions Process.
 - (1) Discovery. Discovery is governed by Rule 190.2.
 - (2) Trial Setting; Continuances. Cn any party's request, the court must set the case for a trial date that is within 90 days after the discovery period in Rule 190.2(b)(1) ends. The court may continue the case twice, not to exceed a total of 60 days.
 - (3) Time Limits for Trial. Each side is allowed no more than eight hours to complete jury selection, opening statements, presentation of evidence, examination and cross-examination of witnesses, and closing arguments. On motion and a showing of good cause by any party, the court may extend the time limit to no more than twelve hours per side.
 - (A) The term "side" has the same definition set out in Rule 233.
 - (B) Time spent on objections, bench conferences, bills of exception, and challenges for cause to a juror under Rule 228 are not included in the time limit.

Misc. Docket 20-9101

- (4) Alternative Dispute Resolution.
 - (A) Unless the parties have agreed not to engage in alternative dispute resolution, the court may refer the case to an alternative dispute resolution procedure once, and the procedure must:
 - (i) not exceed a half-day in duration, excluding scheduling time;
 - (ii) not exceed a total cost of twice the amount of applicable civil filing fees; and
 - (iii) be completed no later than 60 days before the initial trial setting.
 - (B) The court must consider objections to the referral unless prohibited by statute.
 - (C) The parties may agree to engage in alternative dispute resolution other than that provided for in (A).
- (5) Expert Testimony. Unless requested by the party sponsoring the expert, a party may only challenge the admissibility of expert testimony as an objection to summary judgment evidence under Rule 166a or during the trial on the merits. This paragraph does not apply to a motion to strike for late designation.

Comment to 2021 change: Rule 169 is amended to implement section 22.004(h-1) of the Texas Government Code—which calls for rules to promote the prompt, efficient, and cost-effective resolution of civil actions filed in county courts at law in which the amount in controversy does not exceed \$250,000—and changes to section 22.004(h) of the Texas Government Code. Certain actions are exempt from Rule 169's application by statute. *See e.g.*, TEX. ESTATES CODE §§ 53.107, 1053.105.

RULE 190. DISCOVERY LIMITATIONS

190.1 Discovery Control Plan Required.

Every case must be governed by a discovery control plan as provided in this Rule. A plaintiff must allege in the first numbered paragraph of the original petition whether discovery is intended to be conducted under Level 1, 2, or 3 of this Rule.

190.2 Discovery Control Plan - Expedited Actions and Divorces Involving \$50,000250,000 or Less (Level 1)

- (a) Application. This subdivision applies to:
 - (1) any suit that is governed by the expedited actions process in Rule 169; and

Misc. Docket 20-9101

- (2) unless the parties agree that rule 190.3 should apply or the court orders a discovery control plan under Rule 190.4, any suit for divorce not involving children in which a party pleads that the value of the marital estate is more than zero but not more than \$50,000250,000.
- (b) Limitations. Discovery is subject to the limitations provided elsewhere in these rules and to the following additional limitations:
 - (1) Discovery period. All discovery must be conducted during the discovery period, which begins when the suit is filedinitial disclosures are due and continues until 180 days after the date the first request for discovery of any kind is served on a party initial disclosures are due.
 - (2) Total time for oral depositions. Each party may have no more than six20 hours in total to examine and cross-examine all witnesses in oral depositions. The parties may agree to expand this limit up to ten hours in total, but not more except by court order. The court may modify the deposition hours so that no party is given unfair advantage.
 - (3) Interrogatories. Any party may serve on any other party no more than 15 written interrogatories, excluding interrogatories asking a party only to identify or authenticate specific documents. Each discrete subpart of an interrogatory is considered a separate interrogatory.
 - (4) Requests for Production. Any party may serve on any other party no more than 15 written requests for production. Each discrete subpart of a request for production is considered a separate request for production.
 - (5) **Requests for Admissions.** Any party may serve on any other party no more than 15 written requests for admissions. Each discrete subpart of a request for admission is considered a separate request for admission.
 - (6) Requests for Disclosure. In addition to the content subject to disclosure under Rule 194.2, a party may request disclosure of all documents, electronic information, and tangible items that the disclosing party has in its possession, custody or control and may use to support its claims or defenses. A request for disclosure made pursuant to this paragraph is not considered a request for production.
- (c) Reopening Discovery. If a suit is removed from the expedited actions process in Rule 169 or, in a divorce, the filing of a pleading renders this subdivision no longer applicable, the discovery period reopens, and discovery must be completed within the limitations provided in Rules 190.3 or 190.4, whichever is applicable. Any person previously deposed may be redeposed. On motion of any party, the court should continue the trial date if necessary to permit completion of discovery.

190.3 Discovery Control Plan - By Rule (Level 2)

Misc. Docket 20-9101

- (a) **Application.** Unless a suit is governed by a discovery control plan under Rules 190.2 or 190.4, discovery must be conducted in accordance with this subdivision.
- (b) **Limitations.** Discovery is subject to the limitations provided elsewhere in these rules and to the following additional limitations:
 - Discovery period. All discovery must be conducted during the discovery period, which begins when suit is filedinitial disclosures are due and continues until:
 - (A) 30 days before the date set for trial, in cases under the Family Code; or
 - (B) in other cases, the earlier of
 - (i) 30 days before the date set for trial, or
 - (ii) nine months after the earlier of the date of the first oral deposition or the due date of the first response to written discoveryinitial disclosures are due.
 - (2) Total time for oral depositions. Each side may have no more than 50 hours in oral depositions to examine and cross-examine parties on the opposing side, experts designated by those parties, and persons who are subject to those parties' control. "Side" refers to all the litigants with generally common interests in the litigation. If one side designates more than two experts, the opposing side may have an additional six hours of total deposition time for each additional expert designated. The court may modify the deposition hours and must do so when a side or party would be given unfair advantage.
 - (3) Interrogatories. Any party may serve on any other party no more than 25 written interrogatories, excluding interrogatories asking a party only to identify or authenticate specific documents. Each discrete subpart of an interrogatory is considered a separate interrogatory.

* * *

Comment to 2021 change: Rule 190.2 is amended to implement section 22.004(h-1) of the Texas Government Code, which calls for rules "to promote the prompt, efficient, and cost-effective resolution of civil actions filed in county courts at law in which the amount in controversy does not exceed \$250,000" that "balance the need for lowering discovery costs in these actions against the complexity of and discovery needs in these actions." Under amended Rule 190.2, Level 1 discovery limitations now apply to a broader subset of civil actions: expedited actions under Rule 169, which is also amended to implement section 22.004(h-1) of the Texas Government Code, and divorces not involving children in which the value of the marital estate is not more than \$250,000. Level 1 limitations are revised to impose a twenty-hour limit on oral deposition. Disclosure requests under Rule 190.2(b)(6) and Rule 194 are now replaced by required disclosures under Rule

Misc. Docket 20-9101
194, as amended. The discovery periods under Rules 190.2(b)(1) and 190.3(b)(1) are revised to reference the required disclosures.

RULE 192. PERMISSIBLE DISCOVERY: FORMS AND SCOPE; WORK PRODUCT; PROTECTIVE ORDERS; DEFINITIONS

192.1 Forms of Discovery.

Permissible forms of discovery are:

- (a) requests forrequired disclosures;
- (b) requests for production and inspection of documents and tangible things;
- (c) requests and motions for entry upon and examination of real property;
- (d) interrogatories to a party;
- (e) requests for admission;
- (f) oral or written depositions; and
- (g) motions for mental or physical examinations.

192.2 Timing and Sequence of Discovery.

- (a) **Timing.** Unless otherwise agreed to by the parties or ordered by the court, a party cannot serve discovery until after the initial disclosures are due.
- (b) <u>Sequence</u>. The permissible forms of discovery may be combined in the same document and may be taken in any order or sequence.

* * *

192.7 Definitions.

As used in these rules

- (a) Written discovery means requests for required disclosures, requests for production and inspection of documents and tangible things, requests for entry onto property, interrogatories, and requests for admission.
- (b) *Possession, custody, or control* of an item means that the person either has physical possession of the item or has a right to possession of the item that is equal or superior to the person who has physical possession of the item.

Misc. Docket 20-9101

- (c) A *testifying expert* is an expert who may be called to testify as an expert witness at trial.
- (d) A *consulting expert* is an expert who has been consulted, retained, or specially employed by a party in anticipation of litigation or in preparation for trial, but who is not a testifying expert.

RULE 193. WRITTEN DISCOVERY: RESPONSE; OBJECTION; ASSERTION OF PRIVILEGE; SUPPLEMENTATION AND AMENDMENT; FAILURE TO TIMELY RESPOND; PRESUMPTION OF AUTHENTICITY

193.1 Responding to Written Discovery; Duty to Make Complete Response.

A party must respond to written discovery in writing within the time provided by court order or these rules. When responding to written discovery, a party must make a complete response, based on all information reasonably available to the responding party or its attorney at the time the response is made. The responding party's answers, objections, and other responses must be preceded by the request <u>or required disclosure</u> to which they apply.

* * *

193.3 Asserting a Privilege

A party may preserve a privilege from written discovery in accordance with this subdivision.

- (a) Withholding privileged material or information. A party who claims that material or information responsive to written discovery is privileged may withhold the privileged material or information from the response. The party must state—in the response (or an amended or supplemental response) or in a separate document—that:
 - (1) information or material responsive to the request <u>or required disclosure</u> has been withheld,
 - (2) the request or required disclosure to which the information or material relates, and
 - (3) the privilege or privileges asserted.
- (b) Description of withheld material or information. After receiving a response indicating that material or information has been withheld from production, the<u>a</u> party seeking discovery may serve a written request that the withholding party identify the information and material withheld. Within 15 days of service of that request, the withholding party must serve a response that:
 - (1) describes the information or materials withheld that, without revealing the privileged information itself or otherwise waiving the privilege, enables other parties to assess the applicability of the privilege, and

Misc. Docket 20-9101

- (2) asserts a specific privilege for each item or group of items withheld.
- (c) **Exemption.** Without complying with paragraphs (a) and (b), a party may withhold a privileged communication to or from a lawyer or lawyer's representative or a privileged document of a lawyer or lawyer's representative
 - (1) created or made from the point at which a party consults a lawyer with a view to obtaining professional legal services from the lawyer in the prosecution or defense of a specific claim in the litigation in which discovery is requested or required, and
 - (2) concerning the litigation in which the discovery is requested or required.
- (d) **Privilege not waived by production.** A party who produces material or information without intending to waive a claim of privilege does not waive that claim under these rules or the Rules of Evidence if—within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made—the producing party amends the response, identifying the material or information produced and stating the privilege asserted. If the producing party thus amends the response to assert a privilege, the requestingany party who has optained the specific material or information must promptly return the specified material or information and any copies pending any ruling by the court denying the privilege.

193.4 Hearing and Ruling on Objections and Assertions of Privilege.

- (a) Hearing. Any party may at any reasonable time request a hearing on an objection or claim of privilege asserted under this rule. The party making the objection or asserting the privilege must present any evidence necessary to support the objection or privilege. The evidence may be testimony presented at the hearing or affidavits served at least seven days before the hearing or at such other reasonable time as the court permits. If the court determines that an *in camera* review of some or all of the requested discovery <u>or required disclosure</u> is necessary, that material or information must be segregated and produced to the court in a sealed wrapper within a reasonable time following the hearing.
- (b) Ruling. To the extent the court sustains the objection or claim of privilege, the responding party has no further duty to respond to that request or required disclosure. To the extent the court overrules the objection or claim of privilege, the responding party must produce the requested or required material or information within 30 days after the court's ruling or at such time as the court orders. A party need not request a ruling on that party's own objection or assertion of privilege to preserve the objection or privilege.
- (c) Use of material or information withheld under claim of privilege. A party may not use—at any hearing or trial—material or information withheld from discovery under a claim of privilege, including a claim sustained by the court, without timely amending or supplementing the party's response to that discovery.

* * *

Misc. Docket 20-9101

RULE 194. REQUESTS FOR REQUIRED DISCLOSURES

194.1 Request Duty to Disclose; Production.

A party may obtain disclosure from another party of the information or material listed in Rule 194.2 by serving the other party- no later than 30 days before the end of any applicable discovery period the following request: "Pursuant to Rule 194, you are requested to disclose, within 30 days of service of this request; the information or material described in Rule [state rule, *e.g.*, 194.2, or 194.2(a), (c), and (f), or 194.2(d)-(g)]."

- (a) Duty to Disclose. Except as exempted by Rule 194.2(d) or as otherwise agreed by the parties or ordered by the court, a party must, without awaiting a discovery request, provide to the other parties the information or material described in Rule 194.2, 194.3, and 194.4.
- (b) Production. Copies of documents and other tangible items ordinarily must be served with the response. But if the responsive documents are voluminous, the response must state a reasonable time and place for the production of documents. The responding party must produce the documents at the time and place stated, unless otherwise agreed by the parties or ordered by the court, and must provide the requesting party a reasonable opportunity to inspect them.

194.2 ContentInitial Disclosures.

- (a) Time for Initial Disclosures. A party must make the initial disclosures at or within 30 days after the filing of the first answer unless a different time is set by the parties' agreement or court order. A party that is first served or otherwise joined after the filing of the first answer must make the initial disclosures within 30 days after being served or joined, unless a different time is set by the parties' agreement or court order.
- (b) Content. Without awaiting a discovery request. As party may request disclosure of any or all of the followingmust provide to the other parties:
 - (a1) the correct names of the parties to the lawsuit;
 - (b2) the name, address, and telephone number of any potential parties;
 - (e3) the legal theories and, in general, the factual bases of the responding party's claims or defenses (the responding party need not marshal all evidence that may be offered at trial);
 - (d4) the amount and any method of calculating economic damagesa computation of each category of damages claimed by the responding party—who must also make available for inspection and copying the documents or other evidentiary material, unless privileged or protected from disclosure, on which each computation is based, including materials bearing on the nature and extent of injuries suffered;

Misc. Docket 20-9101

- (e5) the name, address, and telephone number of persons having knowledge of relevant facts, and a brief statement of each identified person's connection with the case;
- (6) a copy—or a description by caregory and location—of all documents, electronically stored information, and tangible things that the responding party has in its possession, custody, or control, and may use to support its claims or defenses, unless the use would be solely for impeachment;
- (f) for any testifying expert:
 - (1) the expert's name, address, and telephone number;
 - (2) the subject matter on which the expert will testify;
 - (3) the general substance of the expert's mental impressions and opinions and a brief summary of the basis for them, or if the expert is not retained by, employed by, or otherwise subject to the control of the responding party, documents reflecting such information.
 - (4) if the expert is retained by, employed by, or otherwise subject to the control of the responding party:
 - (A) all documents, tangible things, reports, models, or data compilations that have been provided to, reviewed by, or prepared by or for the expert in anticipation of the expert's testimony; and
 - (B) the expert's current resume and bibliography;
- (g7) any indemnity and insuring agreements described in Rule 192.3(f);
- (h8) any settlement agreements described in Rule 192.3(g);
- (i9) any witness statements described in Rule 192.3(h);
- (j10) in a suit alleging physical or mental injury and damages from the occurrence that is the subject of the case, all medical records and bills that are reasonably related to the injuries or damages asserted or, in lieu thereof, an authorization permitting the disclosure of such medical records and bills;
- (k11) in a suit alleging physical or mental injury and damages from the occurrence that is the subject of the case, all medical records and bills obtained by the responding party by virtue of an authorization furnished by the requesting party; and
- (412) the name, address, and telephone number of any person who may be designated as a responsible third party.

Misc. Docket 20-9101

(c) Content in Certain Suits Under the Family Code.

- (1) In a suit for divorce or annulment, a party must, without awaiting a discovery request, provide to the other party a copy of:
 - (A) all documents pertaining to real estate;
 - (B) all documents pertaining to any pension, retirement, profit-sharing, or other employee benefit plan, including the most recent account statement for any plan;
 - (C) all documents pertaining to any life, casualty, liability, and health insurance; and
 - (D) the most recent statement pertaining to any account at a financial institution, including banks, savings and loans institutions, credit unions, and brokerage firms.
- (2) In a suit in which child or spousal support is at issue, a party must, without awaiting a discovery request, provide to the other party a copy of:
 - (A) all policies, statements, and the summary description of benefits for any medical and health insurance coverage that is or would be available for the child or the spouse;
 - (B) the party's income tax returns for the previous two years or, if no return has been filed, the party's Form W-2, Form 1099, and Schedule K-1 for such years; and
 - (C) the party's two most recent payroll check stubs.
- (d) **Proceedings Exempt from Initial Disclosure.** The following proceedings are exempt from initial disclosure, but a court may order the parties to make particular disclosures and set the time for disclosure:
 - (1) an action for review on an administrative record;
 - (2) a forfeiture action arising from a state statute; and
 - (3) a petition for habeas corpus.

194.3 Response.

The responding party must serve a written response on the requesting party within 30 days after service of the request, except that:

Misc. Docket 20-9101

(a) a defendant served with a request before the defendant's answer is due need not respond until 50 days after service of the request, and

(b) a response to a request under Rule 194.2(f) is governed by Rule 195.

194.3 Testifying Expert Disclosures.

In addition to the disclosures required by Rule 194.2, a party must disclose to the other parties testifying expert information as provided by Rule 195.

194.4 Production.

Copies of documents and other tangible iteras ordinarily must be served with the response. But if the responsive documents are voluminous, the response must state a reasonable time and place for the production of documents. The responding party must produce the documents at the time and place stated, unless otherwise agreed by the parties or ordered by the court, and must provide the requesting party a reasonable opportunity to inspect them.

194.4 Pretrial Disclosures.

- (a) In General. In addition to the disclosures required by Rule 194.2 and 194.3, a party must provide to the other parties and promptly file the following information about the evidence that it may present at trial other than solely for impeachment:
 - (1) the name and, if not previously provided, the address, and telephone number of each witness—separately identifying those the party expects to present and those it may call if the need arises;
 - (2) an identification of each document or other exhibits, including summaries of other evidence—separately identifying those items the party expects to offer and those it may offer if the need arises.
- (b) Time for Pretrial Disclosures. Unless the court orders otherwise, these disclosures must be made at least 30 days before trial.

194.5 No Objection or Assertion of Work Product.

No objection or assertion of work product is permitted to a requestdisclosure under this rule.

194.6 Certain Responses Not Admissible.

A response to requests disclosure under Rule 194.2(eb)(3) and (d4) that has been changed by an amended or supplemental response is not admissible and may not be used for impeachment.

Comment to 2021 change: Rule 194 is amended to implement section 22.004(h-1) of the Texas Government Code, which calls for rules "to promote the prompt, efficient, and cost-effective

Misc. Docket 20-9101

resolution of civil actions filed in county courts at law in which the amount in controversy does not exceed \$250,000" that "balance the need for lowering discovery costs in these actions against the complexity of and discovery needs in these actions." Rule 194 is amended based on Federal Rule of Civil Procedure 26(a) to require disclosure of basic discovery automatically, without awaiting a discovery request. A party is not excused from making its disclosures because it has not fully investigated the case or because it challenges the sufficiency of another party's disclosures or because another party has not made its disclosures. As with other written discovery responses, required disclosures must be signed under Rule 191.3, complete under Rule 193.2, served under Rule 191.5, and timely amended or supplemented under Rule 193.5.

RULE 195. DISCOVERY REGARDING TESTIFYING EXPERT WITNESSES

195.1 Permissible Discovery Tools.

A party may request another party to designate and disclose <u>obtain</u> information concerning testifying expert witnesses only through a request for disclosure under Rule 194 and this rule and through depositions and reports as permitted by this rule.

195.2 Schedule for Designating Experts.

Unless otherwise ordered by the court, a party must designate experts—that is, furnish information requested underdescribed in Rule 194.2(f)195.5(a)—by the later of the following two-dates: 30 days after the request is served, or

- (a) with regard to all experts testifying for a party seeking affirmative relief, 90 days before the end of the discovery period;
- (b) with regard to all other experts, 60 days before the end of the discovery period.

* * *

195.4 Oral Deposition.

In addition to the information disclosureed under Rule 1945.5(a), a party may obtain discovery concerning the subject matter on which the expert is expected to testify, the expert's mental impressions and opinions, the facts known to the expert (regardless of when the factual information was acquired) that relate to or form the basis of the testifying expert's mental impressions and opinions, and other discoverable matters, including documents not produced in disclosure, only by oral deposition of the expert and by a report prepared by the expert under this rule.

195.5 Court Ordered Expert Disclosures and Reports.

- (a) **Disclosures**. Without awaiting a discovery request, a party must provide the following for any testifying expert:
 - (1) the expert's name, address, and telephone number;

Misc. Docket 20-9101

- (2) the subject matter on which the expert will testify;
- (3) the general substance of the expert's mental impressions and opinions and a brief summary of the basis for them, or if the expert is not retained by, employed by, or otherwise subject to the control of the responding party, documents reflecting such information;
- (4) if the expert is retained by, employed by, or otherwise subject to the control of the responding party:
 - (A) all documents, tangible things, reports, models, or data compilations that have been provided to, reviewed by, or prepared by or for the expert in anticipation of the expert's testimony;
 - (B) the expert's current resume and bibliography;
 - (C) the expert's qualifications, including a list of all publications authored in the previous 10 years;
 - (D) a list of all other cases in which, during the previous four years, the expert testified as an expert at trial or by deposition; and
 - (E) a statement of the compensation to be paid for the expert's study and testimony in the case.
- (b) <u>Expert Reports.</u> If the discoverable factual observations, tests, supporting data, calculations, photographs, or opinions of an expert have not been recorded and reduced to tangible form, the court may order these matters reduced to tangible form and produced in addition to the deposition.

Comment to 2021 change: Rule 195 is amended to reflect changes to Rule 194. Amended Rule 195.5(a) lists the disclosures for any testifying expert, which are now required without awaiting a discovery request, that were formerly listed in Rule 194(f). Amended Rule 195.5(a) also includes three new disclosures based on Federal Rule of Civil Procedure 26(a)(2)(B).

Misc. Docket 20-9101

^{* * *}



Statutes and Rules Cited

[References are to sections in the text.]

TEXAS

Texas Business & Commerce Code

§ 72.002	 § 72.003	1.3

Texas Civil Practice & Remedies Code

§ 41.0115(b)	. 24.6:3	\$ 74.052	24 6.1
g 41.0115(0)	. 24.6:3	§ 74.052	24.6:

Texas Government Code

§§ 552.001–.353 24.6:2

Texas Occupations Code

§ 159.002(a)24.7	§ 201.404	. 24.6:2
§ 201.205	§ 201.405	. 24.6:2

Texas Penal Code

§ 32.51	§ 33.07
§ 33.02	§ 43.26
§ 33.021	§ 43.261

Texas Rules of Civil Procedure

Rule 1 9.2:3	Rule 21a 21.5:2
Rule 11 19.3:4	Rule 109 21.5:2

Rule 171 12.8
Rule 176.4 21.2:2
Rule 176.7
Rule 190.2(b)(2) 16.2:4
Rule 190.3(b)(2) 16.2:4
Rule 190.4(b) 16.2:4
Rule 191.2 13.3:1
Rule 191.3 13.3:2
Rule 192.3 8.9:1
Rule 192.3(a) 8.9:1, 13.3:2
Rule 192.3(b) 8.9:1, 16.3:1
Rule 192.4 13.3:1, 13.3:2
Rule 192.4(b) 13.3:3, 21.9:4
Rule 192.5 13.3:3
Rule 192.5(a) 8.10:2
Rule 192.5(a)(1) 8.10:2
Rule 192.5(b)(1) 8.10:2
Rule 192.5(b)(2) 8.10:2
Rule 192.6 13.3:2, 13.3:3
Rule 192.6(a) 16.3:3
Rule 192.6(b) 13.3:1
Rule 192.7 1.2
Rule 193.1 13.3:3
Rule 193.2(a)–(e) 13.3:3
Rule 193.2(f) 13.3:3
Rule 193.3 12.8, 13.3:3
Rule 193.3(d) 12.2, 19.2:3, 25.8:6
Rule 193.4 13.3:3
Rule 193.4(a) 13.3:1
Rule 193.4(b) 13.3:1
Rule 193.7 18.2:3, 18.2:4
Rule 193.3(d) cmt. 4 12.2
Rule 194.6 14.1

Rule 196	14.4:1
Rule 196.2	9.2:4
Rule 196.3(c)	9.2:5
Rule 196.4 9.2, 9.2	::1, 9.2:2, 13.3:1,
	14.4, 21.3, 21.4
Rule 196.6	13.3:3
Rule 196.7(a)	
Rule 196.7(b)	21.7, 21.11
Rule 196 cmt. 3	14.4:3
Rule 199.2	21.2:3
Rule 199.2(a)	21.2:3
Rule 199.2(b) 16.2	:1, 21.2:3, 21.2:4
Rule 199.2(b)(1) 16.2	:2, 16.4:1–16.4:4
Rule 199.2(b)(5)	21.2:3
Rule 199.5	21.2:3
Rule 199.5(c)	16.4:1
Rule 199.5(f)	16.4:4
Rule 200.1	21.2:3
Rule 200.1(a)	21.2:3
Rule 200.1(b)	21.2:3
Rule 200.3	21.2:3
Rule 200.4	21.2:3
Rule 202.1	
Rule 202.2	21.5:1
Rule 202.3(a)	21.5:2
Rule 202.3(b)	21.5:2
Rule 202.3(d)	21.5:2
Rule 202.4(b)	21.5:3
Rule 202.5	5, 21.5:4, 21.10:3
Rule 204.1	
Rule 204.2(a)	
Rule 205.1	21.2:1
Rule 205.1(c)	21.2:3

Statutes and Rules Cited

Texas Disciplinary Rules of Professional Conduct

Rule 205.2	21.2:1, 21.2:3, 21.2:4	Rul
Rule 205.3		Rul
Rule 205.3(a)		Rul

Rule 205.3(b)	•	•	•	•		•	•	•	•		•		2	21.2:4	
Rule 205.3(b)(3)		•		•					•	•				.21.4	
Rule 205.3(f)											•			.21.3	

Texas Rules of Evidence

18.3:2
18.2:2
6:2, 13.3:2
24.6:1
24.6:1
18.3:6
18.3:2
18.3:2
18.3:2
18.3:5
18.3:2
18.3:2

Rule 803(1) 18.3:3
Rule 803(2) 18.3:3
Rule 803(3) 18.3:3
Rule 803(5) 18.3:4
Rule 803(6) 18.3:4
Rule 803(17) 18.3:4
Rule 804 18.3:2
Rule 901 18.2, 20.7
Rule 901(b)(5) 18.2:22
Rule 901(b)(9) 18.2:18
Rule 1001(d) 18.3:1
Rule 1002 18.3:1
Rule 1004 18.3:1

Texas Disciplinary Rules of Professional Conduct

Rule $1.01(a)(1) \dots 19.2:2, 19.$	3:1
Rule 1.01(b)(1) 19.	2:5
Rule 1.01(c) 19.	2:5
Rule 1.01 cmt. 6 19.	4:1
Rule 1.02(a)(1)19.	2:4
Rule 1.02(c) 19.	2:4
Rule 1.02(f)19.	2:4
Rule 1.04(f)19.	3:3
Rule 1.04 cmt. 10	3:3
Rule 1.04 cmt. 12 19.	3:3
Rule 1.05(b) 19.	4:1

. 19.2:3
. 19.2:4
. 19.2:4
. 19.4:1
. 19.4:2
. 19.4:1
. 19.4:1
. 19.4:2
. 19.4:1
25.8:7
25.8:3

Texas Disciplinary Rules of Professional Conduct

Essentials of E-Discovery

Rule 4.04(a)	19.2:1	Rule 5.02	19.3:2
Rule 5.01	19.3:2		

UNITED STATES

United States Code

Title 18	Title 28
§ 1001 23.4:6	§ 636(b)(1)(A) 25.2
§ 1503(a)	§ 1920 14.1, 14.3
§ 251024.5	§ 1920(4) 14.3
§ 2721	Title 42
§ 3509(m) 25.7:3	§ 1320d24.5
Title 20	Title 47
§ 1232	§ 55124.5

Code of Federal Regulations

Title 45	§ 512(e)
§ 160	

Federal Rules of Civil Procedure

Rule 1
Rule 5.2(a)(2) 24.2:3
Rule 5.2(d)
Rule 9.10(c) 24.3:1
Rule 9.10(d)
Rule 9.10(g)
Rule 1612.6
Rule 16(b)(1) 6.2:4
Rule 16(b)(3)(B)(iii–iv) 6.2:4
Rule 16(b)(3)(B)(iv)12.6

Rule 21c(a) 24	4.3:1
Rule 21c(b) 24	4.3:1
Rule 21c(c) 24	4.3:1
Rule 21c(d) 24	4.3:1
Rule 21c(f) 24	4.3:1
Rule 26 1.7, 6.1, 13.2:1, 14.2:2, 1	6.3:1
Rule 26(a)(1)(A)(ii) 1	9.2:2
Rule 26(b)(1) 8.2:2, 8.9:1, 13 13.2:2, 14.2:2, 16.3:1, 2	.2:1,
Rule 26(b)(2) 2.5, 14.1, 1	4.2:2

24.5

Rule 26(b)(2)(B) 3.6, 6.4, 6.7, 8.9:1, 13.2:1, 14.2:2, 19.2:2, 21.9:4
Rule 26(b)(2)(C)13.2:1, 13.2:3, 14.2:2
Rule 26(b)(2)(C)(i)
Rule 26(b)(2)(C)(iii) 8.9:2, 14.2:4
Rule 26(b)(2)(D)
Rule 26(b)(4)6.6:5
Rule 26(b)(5)(A)13.2:2
Rule 26(b)(5)(B) 6.2:4, 12.5
Rule 26(c) 14.2:2, 24.2:2
Rule 26(c)(1) 13.2:3, 16.3:3, 23.2:3, 23.4:2
Rule 26(c)(1)(A)–(H)
Rule 26(c)(1)(B) 14.2:2
Rule 26(c)(1)(D) 13.2:3
Rule 26(c)(2)13.2:3
Rule 26(c)(3)13.2:3, 16.3:3
Rule 26(d)(2)6.2:4, 13.2:2
Rule 26(e)
Rule 26(f) 3.6, 6.1, 6.2:4, 6.3–6.5, 6.7, 6.8, 16.3:1, 19.2:2
Rule 26(f)(1) 6.1, 6.2:1
Rule $26(f)(2)-(3)$ 6.2:4
Rule 26(f)(2) 1.7, 6.2:2–6.2:4
Rule 26(f)(3)(A) 6.2:4
Rule 26(f)(3)(B)6.2:4
Rule 26(f)(3)(C) 1.7, 5.8, 6.1, 6.2:4
Rule $26(f)(3)(D) \dots 6.2:4, 12.6$
Rule $26(f)(3)(E) \dots 6.2:4$
Rule $26(f)(3)(F)$ $6.2:4$
Rule 26(g)
Rule 26(g)(1) 6.8, 13.2:1, 13.2:2
Rule 26(g)(1)(B) 13.2:1, 13.2:3
Rule 26(g)(3)13.2:1, 13.2:3

Rule 27(a)(1)	
Rule 27(a)(2)	
Rule 27(a)(3)	
Rule 27(a)(4)	
Rule 29	
Rule 30	16.2:4, 16.4:1
Rule 30(a)(2)	
Rule 30(a)(2)(A)(ii) .	
Rule 30(b)(6)	16.2:1, 16.4:1–16.4:4
Rule 30(c)(2)	
Rule 30(d)(1)	
Rule 34	1.9, 6.3, 9.3:3–9.3:5,
	12.7, 14.4:1
Rule 34(a)	1.12, 6.6:3, 13.2:2
Rule 34(b)	
Rule $34(b)(1) \dots$	
Rule $34(b)(1)(A)$	
Rule $34(b)(1)(C)$	6.3, 9.3:3
Rule 34(b)(2)(B)–(C)	
Rule $34(b)(2)(B)$	
Rule $34(b)(2)(C)$	
Rule 34(b)(2)(C)(i)	
Rule $34(b)(2)(E) \dots$	
Rule $34(b)(2)(E)(i)$	
Rule 34(b)(2)(E)(ii) .	9.3:2, 9.3:4, 9.4:3
Rule 34(b)(2)(E)(iii).	
Rule 34(c)	
Rule 37	1.8, 1.9, 2.4:1, 6.8
Rule 37(a)	13.2:3
Rule 37(a)(3)(B)(iv).	13.2:3
Rule 37(a)(4)	13.2:3
Rule 37(a)(5)	16.3:3
Rule $37(a)(5)(A)$	

Federal Rules of Civil Procedure

Rule 37(a)(5)(B)–(C) 13.2:3	Rule 45(d) 21.9:2
Rule 37(a)(5)(B) 13.2:3	Rule 45(d)(1) 13.2:4, 21.9:2
Rule 37(b)(2)(A) 14.2:6	Rule 45(d)(2)(A) 13.2:4, 21.9:3
Rule 37(c)(1)(A) 14.2:6	Rule 45(d)(2)(B)–(C)
Rule 37(e) 2.2, 15.2:2, 15.4	Rule 45(d)(2)(B) 13.2, 13.2:4, 21.9:2
Rule 37(e)(1) 15.2:8	Rule 45(d)(2)(B)(ii) 13.2:4, 21.9
Rule 37(e)(2) 15.2:11	Rule 45(d)(3)(A) 13.2, 13.2:4, 21.9
Rule 45 13.2	Rule 45(e)(1) 13.2:4, 21.9
Rule 45(a)(1)(A)(iii) 21.9:1	Rule 45(e)(1)(B) 21.9:3
Rule 45(a)(1)(C) 13.2:4, 21.9, 21.9:1, 21.9:3	Rule 45(e)(1)(C)
Rule 45(a)(2) 21.9:2	Rule 45(e)(1)(D) 21.9:4
Rule 45(c)(1) 21.9:3	Rule 53 12.8
Rule 45(c)(2)(A) 21.9:3	Rule 54(d) 14.1
Rule 45(c)(2)(B) 13.2, 21.9	Rule 76a(a) 24.3:2
Rule 45(c)(3)(A)(iv) 13.2, 21.9	Rule 192.6(b)

Federal Rules of Evidence

Rule 502 6.2:4, 6.5,	Rule 502(d) 12.6, 12.8
12.4, 19.2:3, 26.1:11	Rule 901(b)(9) 18.2:20
Rule 502(b) 12.4, 12.4:3	Rule 902(13)
Rule 502(b)(2) 12.4:2	Rule 902(14)

Cases Cited

[References are to sections in the text.]

A

Abbott v. Texas Dept. of Mental Health & Mental Retardation, 24.6:2 Abilify (Aripiprazole) Prod. Liab. Litig. [In re], 15.2:4 Abraham v. Cavender Boerne Acquisition of Texas, Ltd., 20.2 Activision Blizzard, Inc. [In re], 23.3:2 Actos (Pioglitazone) Prod. Liab. Litig [In re], 10.11, 10.13 Adair v. EQT Production Company, 14.2:4 Adidas Am., Inc. v. TRB Acquisitions LLC, 16.4:3 Adobe Land Corp. v. Griffin, L.L.C., 1.6:2 Advanced Powder Solutions, Inc. [In re], 1.5:2, 15.3:11 Advocat "Christopher X" [In re], 23.3:2 Aguilar v. Immigration & Customs Enforcement Div. of U.S. Dep't of Homeland Sec., 6.3, 19.3:4 AHF Comm. Dev., LLC v. City of Dallas, 12.4:3 A.H.J. [In re], 15.3:11 A.I. Credit Corp. v. Legion Ins. Co., 16.2:3 Alabama Aircraft Indus., Inc. v. Boeing Co., 15.2:11 Alers v. City of Philadelphia, 12.4:2, 12.4:3 Alford Chevrolet-Geo [In re], 13.3:2, 13.3:3 Allstate County Mut. Ins. Co. [In re], 13.3:2

Allstate Tex. Lloyds v. Johnson, 16.2:2 Alston v. City of Darien, 15.2:8 Alston v. Park Pleasant, Inc., 15.2:11 Alyeska Pipeline Service Co. v. Widerness Society, 14.2:1 American Airlines, Inc. v. Travelport Limited, 13.2:1 Am. Fed'n of Musicians of the U.S. & Canada v. SKODAM Films, LLC, 13.2:4, 21.9 Amobi v. Dist. of Columbia Dep't of Corr., 12.4:1, 12.4:2 Anderson Living Trust v. WPX Energy Prod., LLC, 9.3:2 Andra Group, LP v. JDA Software Group, Inc., 13.2, 13.2:4, 21.9, 21.9:2 Anschuetz & Co. [In re], 23.2:2 A.O.A. v. Rennert, 15.2:4 Archer v. York City Sch. Dist., 15.2:11 Arenson v. Whitehall Convalescent & Nursing Home, Inc., 24.2:2 Arnold [In re], 24.6:3 Arthur J. Gallagher & Co. v. O'Neill, 13.2, 21.9 Asbestos Prods. Liab. Litig. (No. VI) [In re], 13.2:2 Ashton v. Knight Transportation, Inc., 1.5, 1.9 Assousa v. State, 25.8:6 Astra Aktiebolag v. Andrx Pharmaceuticals, Inc., 23.5:2 Auer v. City of Minot, 15.2:11 Aurora Coop. Elevator Co. v. Aventine Renewable Energy-Aurora W., LLC, 10.13, 10.15, 10.15:1

Auto Club Family Ins. Co. v. Ahner, 13.2:1 Avery v. LPP Mortgage, Ltd., 18.2:2

B

Bailey v. Brookdale Univ. Hosp. Med. Ctr., 14.2:4 Bailey v. State, 18.3:7 Ballard v. Wal-Mart Stores East, LP, 15.2:4 Banargent v. State, 18.2:22 BankDirect Capital Fin., LLC v. Capital Premium Fin., Inc., 15.2:11 Barbera v. Pearson Educ., Inc., 15.2:9 Barcroft Media, Ltd. v. Coed Media Grp., LLC, 15.2:6 Bard IVC Filters Prod. Liab. Litig. [In re], 24.2:1, 24.8 Barnhart v. Morales, 18.3:4 Basra v. Ecklund Logistics, Inc., 15.2:11 Bear Republic Brewing Co. v. Central City Brewing Co., 12.4 Beck [In re], 15.3:11 Bell v. Moawad Grp., LLC, 20.6 Bellamy v. Wal-Mart Stores, Texas, LLC, 12.6 Bellow v. Bellow, 15.3:11 Benicar (Olmesartin) Products Liability Litigation [In re], 9.3:5 Bezerra v. State, 18.3:7 Biomet M2a Magnum Hip Implant Prod. Liab. Litig. [In re], 8.9:2, 10.13, 10.15, 10.15:1 Black v. Callahan, 18.2:5 Blanche v. First Nationwide Mortg. Corp., 18.2:3 Bland v. Roberts, 18.3:7 BMC Software Belgium, N.V. v. Marchand, 20.6 Bohmfalk v. Linwood, 21.2:3

Bowers v. Mortgage Electronic Registration Systems, Inc., 16.4:1 Boxer Prop. Mgmt. Corp. [In re], 16.3:2 BP Expl. & Prod. Inc. v. Cashman Equip. Corp., 18.3:7 Bradley v. State, 20.10 Brady v. Maryland, 25.6, 25.8:3, 25.8:7 Brand Energy & Infrastructure Servs., Inc. v. Irex Corp., 16.3:2 Branum v. State, 25.8:7 Brazos River Auth. v. GE Ionics, Inc., 16.2:4, 16.4:3 Bristol-Myers Squibb Co. v. Superior Court of Cal., 20.6 Broiler Chicken Antitrust Litig. [In re], 8.9:2 Brookshire Bros. v. Aldridge, 1.5:2, 15.3:1-15.3:6, 15.3:8-15.3:11, 15.4 Bro-Tech Corp. v. Thermax, Inc., 22.8:4 Brown v. Bridges, 13.2:3 Brown v. State, 18.2:21 Browning-Ferris Industries, Inc. [In re], 24.3:2 Bruggeman ex rel. Bruggeman v. Blagojevich, 13.2:2 Bryant v. Wal-Mart Louisiana, L.L.C., 15.2:1Bullman v. State, 18.2:12, 20.10 Burnett v. Ford Motor Co., 16.3:2 Butler v. State, 18.2:5, 18.2:9

C

Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 1.5:3, 2.4:2
Calzaturficio S.C.A.R.P.A. v. Fabiano Shoe Co., 16.4:3
Campbell v. State, 18.2:12, 20.7
Campos v. State, 18.3:4
Cannata v. Wyndham Worldwide Corp., 2.4:2, 2.5
Carlson v. Xerox Corp., 19.3:3 Carr v. State Farm Mut. Auto. Ins. Co., 13.2:2, 13.2:3, 13.3:1 Cartel Asset Management v. Ocwen Financial Corp., 6.8 Casey v. Nationstar Mortgage, LLC, 13.2:2 Celexa and Lexapro Products Liability Litigation [In re], 6.4 Cervantez v. State, 25.8:2 Chambers v. NASCO, Inc., 14.2:1 Chapman & Cole v. Itel Container Int'l B.V., 13.2:1 Charalambopoulos v. Grammar, 13.2:3 Chenault v. Dorel Industries, Inc., 14.3 Chen-Oster v. Goldman, Sachs & Co., 14.2:3 Chet Morrison Contractors, Inc. v. Medco Energi US LLC, 9.3:2 Chevron Corp. v. Stratus Consulting, Inc., 6.3 Chin v. Port Authority of New York & New Jersey, 2.4:1, 3.8 Christus Health Southeast Texas [In re], 24.6:1, 24.6:4 Christus Spohn Hospital Kleberg [In re], 12.2 Citgo Petroleum Corp. v. Seachem, 16.5 City of Dickinson [In re], 12.2, 13.3:2 City of Rockford v. Mallinckrodt ARD Inc., 8.9:2 Clark [*In re*], 14.4:2 Clarke v. J.P. Morgan Chase & Co., 12.4:2, 12.4:3 Clean Harbors Environmental Services, Inc. v. ESIS, Inc., 14.2:3 Clientron Corp. v. Devon IT, Inc., 15.2:1 COA Inc. v. Xiamei Houseware Group Co., Inc., 13.2, 21.9 Coble v. State, 18.3:3 Coburn Group, LLC v. Whitecap Advisors, LLC, 12.1, 12.4:1–12.4:3 Coe v. State, 18.2:12

Cofield v. Crumpler, 14.3 Cole's Wexford Hotel, Inc. v. Highmark. Inc., 8.2:2 Colonial Pipeline Co. [In re], 9.2:5 Com. v. Purdy, 18.2:12 Commins v. NES Rental Holdings, Inc., 16.3:1 Comrie v. Ipsco, Inc., 12.4:2 Concerned Citizens v. Belle Haven Club, 16.4:3 Concord Boat Corp. v. Brunswick Corp., 13.2, 21.9 Consumer Electronics Ass'n v. Compras & Buys Magazine, Inc., 13.2:2 Consumer Financial Protection Bureau v. Weltman, Weinberg & Reis, Co., L.P.A., 14.3 Convolve, Inc. v. Compaq Computer Corp., 3.8 Cook v. City of Dallas, 13.2:2 Cook v. State, 18.3:5, 18.3:7 CooperVision, Inc. v. Ciba Vision Corp., 9.3:2 Cordoba v. Pulido, 15.2:9 Cornell Pump Co. v. Thompson Pump Manufacturing Co., 6.8 Correra [In re], 1.2, 15.2:11 Costantino v. City of Atl. City, 14.2:4 Cotracom Commodity Trading Co. v. Seaboard Corp., 13.2:3 Country Vintner of North Carolina, LLC v. E.&J. Gallo Winery, Inc., 14.3 Courtney [In re], 18.3:7 Covad Communications Co. v. Revonet, Inc., 6.3 Crawford v. State, 25.8:7 Crestcare Nursing & Rehabilitation Center [In re], 24.1, 24.6:6 Crispin v. Christian Audigier, Inc., 24.6:4 Crompton Greaves, Ltd. v. Shippers Stevedoring Co., 16.2:3

Essentials of E-Discovery

Crosby v. La. Health Serv. & Indem. Co., 13.2:3
Crosswhite v. Lexington Ins. Co., 13.2:3
Crownover v. Crownover, 13.2:2
Crum & Forster Specialty Ins. Co. v. Great West Casualty Co., 13.2:1
CSX Corp. [*In re*], 13.3:2
Cunningham v. Std. Fire Ins. Co., 16.3:2
Cutting Underwater Techs. USA, Inc. v. ENI U.S. Operating Co., 16.4:4
CV Therapeutics, Inc., Securities Litigation [*In re*], 16.4:2
CyWee Group Ltd. v. Samsung Electronics Co., Ltd., 13.2:2

D

Dahl v. Bain Capital Partners, LLC, 14.4:1 Daimler v. Bauman, 23.2:1 Dale v. Rife, 15.2:11 Da Silva Moore v. Publicis Groupe, 8.12, 10.15:1

Datel Holdings Ltd. v. Microsoft Corp., 12.4:2, 12.4:3

- Davis v. Hinds Cty., Mississippi, 15.2:1
- Davis SR Aviation, LLC v. Rolls-Royce Deutschland Ltd. & Co. KG, 1.6:1, 2.4:1
- De Angelis v. City of El Paso, 13.2:3
- Delapaz v. State, 18.3:3
- DeLeon v. Lacey, 15.3:11
- Dering v. State, 18.2:12, 20.10
- Detoy v. City & County of S.F., 16.4:4
- Deutsche Bank National Trust Company v. Pink, 13.2:1–13.2:3
- Diamond v. State, 18.2:23
- Diamond Triumph Auto Glass, Inc. v. Safelite Glass Corp., 16.2:3

Diesel Machinery, Inc. v. Manitowoc Cranes, Inc., 12.4:2 District Attorney's Office of the 25th Judicial District [In re], 25.8:5 Dizdar v. State Farm Lloyds, 9.3:5 Doe [In re], 18.2:2, 18.2:6 Doe v. Northside I.S.D., 1.5:3 Dolquist v. Heartland Presbytery, 13.2:3 Domville v. State, 20.8 Downing v. Abbott Labs., 16.3:2 Dravo Corp. v. Liberty Mutual Ins. Co., 16.2:1 Duarte v. St. Paul Fire & Marine Insurance Co., 1.2 Durand [In re], 14.2:6 Dwelly v. Yamaha Motor Corp., 16.2:1, 16.4:1 Dynamo Holdings L.P. v. Comm'r, 8.9:2, 10.15, 10.15:1

E

E.A.K. [In re], 18.3:4 Eaton-Stephens v. Grapevine Colleyville Indep. Sch. Dist., 15.2:11 eBay, Inc. v. MercExchange, LLC, 18.3:7 Ebay Seller Antitrust Litigation [In re], 2.5 Edelson v. Cheung, 15.2:11 Eden Isle Marina, Inc. v. United States, 12.4:2, 12.4:3 Edwards v. 4JLJ, LLC, 1.2 EEOC v. Boeing Co., 16.3:2 E.E.O.C. v. GMRI, Inc., 15.2:11 E.E.O.C. v. Simply Storage Management, LLC, 24.6:4 E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc., 2.2, 19.2:5 Emack v. State, 25.8 Enron Sec., Derivative & ERISA Litig. [In re], 19.3:3

Cases Cited

Entrata, Inc. v. Yardi Sys., Inc., 10.13, 10.15.10.15:1 Eolas Technologies, Inc. v. Adobe Systems, Inc., 14.3 EORHB, Inc. v. HOA Holdings LLC, 10.15:5 EPAC Techs., Inc. v. HarperCollins Christian Publ'g, Inc., 15.2:5 EPAC Techs., Inc. v. Thomas Nelson, Inc., 15.2:5 Equal Employment Opportunity Commission v. Methodist Hospitals of Dallas, 13.2:2 Escalona v. State, 18.2:22, 18.2:23 Estate of Shaw v. Marcus, 14.2:2 Ex parte (see name of party) Ex Parte Application of Grupo Mexico SAB de CV [In re], 13.2:4, 21.9 Exxon Corp. [In re], 8.10:2, 16.3:2

F

Fairholme Funds, Inc. v. United States, 12.6 Fannie Mae Sec. Litig. [In re], 19.2:2 F.D.I.C. v. Brudnicki, 14.2:4 Fed. Hous. Fin. Agency v. JPMorgan Chase & Co., 10.13 Fed. Trade Comm'n v. Liberty Supply Co., 14.2:2 Felman Production, Inc. v. Industrial Risk Insurers, 1.12 Ferring B.V. v. Fera Pharms., LLC, 16.3:2 Fidelity & Deposit Co. of Maryland v. McCulloch, 12.3 Finjan, Inc. v. Zscaler, Inc., 24.8 First Am. Bankcard, Inc. v. Smart Bus. Tech., Inc., 13.2:3 First American CoreLogic, Inc. v. Fiserv, Inc., 12.4, 12.4:1 Fischer v. State, 18.3:2, 18.3:3

Fish v. Air & Liquid Sys. Corp., 16.3:2 Fitch v. State, 20.10 Flagstar Bank, FSB v. Walker, 15.3:11 Flanders v. Dzugan, 2.4:1 Flores v. AT&T Corp., 1.5:3 Ford Motor Co. v. Castillo, 13.3:2 Foreclosure Management Co. v. Asset Management Holdings, LLC, 14.2:2 Fowler v. State, 18.2:21 F.P. [In re], 18.1, 18.2:8 Franklin v. State, 18.2:9 Frazier v. Bed Bath & Beyond, Inc., 24.2:2 Freedman v. Weatherford Int'l Ltd., 16.3:2 Friend v. Time Manufacturing Co., 18.5:2 Frierson v. City of Terrell, 24.6:6

G

Gant v. State, 25.8:6 Garcia v. Professional Contract Servs., Inc., 13.2, 21.9 Garcia v. State, 18.3:3 Gardner v. State, 18.2:9 Genentech, Inc. v. Trustees of Univ. of Pa., 13.2:2 GenOn Mid-Atlantic, LLC v. Stone & Webster, Inc., 2.4:1 Ghanam v. Does, 18.3:7 Gibson v. Ford Motor Co., 2.5 Giglio v. United States, 25.6, 25.8:3 Gipson v. Mgmt. & Training Corp., 15.2:1 Global Aerospace Inc. v. Landow Aviation, 10.15:3 GN Netcom, Inc. v. Plantronics, Inc., 7.4:5, 15.2:11 Go v. Rockefeller University, 14.2:3

Essentials of E-Discovery

Goldrich v. City of Jersey City, 15.2:8, 15.2:11 Gondola v. USMD PPM, LLC, 13.2:2 Gonzales v. Pan Am. Labs., L.L.C., 14.3 Gonzalez v. State, 20.10 Goodman v. State, 18.3:3 Goodrich v. State, 18.2:23 Goodyear Tire & Rubber Co. v. Haeger, 15.2:1 GoPro, Inc. v. 360Heros, Inc., 15.2:11 Graves v. Dretke, 25.8:3 Green v. Harris County, Texas, 1.5:3 Grupo Mexico SAB de CV v. SAS Asset Recovery, Ltd., 13.2:4, 21.9 Gutierrez v. Walsh, 21.2:3 Gutman v. Klein, 14.2:6 Guzman v. Jones, 1.5:1

H

Haas v. State, 18.2:16 Hager v. Graham, 13.2:2 Hale v. Richey, 20.6 Hall v. Rent-A-Center, Inc., 13.2:1 Hall v. State, 20.10 Halleen v. Belk, Inc., 13.2:2 Harrison v. Wells Fargo Bank, N.A., 13.2:3 Hawa v. Coatesville Area Sch. Dist., 14.2:2 HCC Ins. Holdings, Inc. v. Flowers, 15.2:11 Heartland Surgical Specialty Hosp., LLC v. Midwest Div., Inc., 16.3:3 H.E.B. Grocery Co., L.P. [In re], 24.6:1 Heller v. City of Dallas, 13.2:1, 13.2:4, 21.9 Henderson v. Union Pac. R.R. Co., 13.2:2 Heng Chan v. Triple 8 Palace, 2.4:2

Heraeus Kulzer, GmbH v. Biomet, Inc., 13.2.21.9 Hines v. State, 18.2:21 Hoagland v. Butcher, 20.6 Hoffman v. L&M Arts, 16.5 Hogan v. Beckel, 21.2:3 Hogg v. Lynch, Chappell & Alsup, P.C., 15.3:11 Holcombe v. Advanced Integration Technology, 13.2:2 Honza [In re], 14.4:2, 21.6 Hopkins v. Green Dot Corp., 13.2:2 Hopson v. Mayor & City Council of Baltimore, 12.1, 12.3 Hsueh v. New York State Dep't of Financial Services, 15.2:1 Hubbard v. Potter, 16.3:2 Hugler v. Sw. Fuel Mgmt., Inc., 15.2:9 Hume v. Consolidated Grain & Barge, Inc., 13.2, 21.9 Hunt Construction Group, Inc. v. Cobb Mechanical Contractors, Inc., 13.2:2, 13.2:3 Hycarbex, Inc. v. Anglo-Suisse, Inc., 21.2:3 Hyles v. New York City, 6.6:2, 6.8, 10.15, 10.15:2, 10.16

I

Illiana Surgery & Medical Center, LLC v. Hartford Fire Insurance Co., 16.5
ILWU-PMA Welfare Plan Bd. of Trustees & ILWU-PMA Welfare Plan v. Connecticut Gen. Life Ins. Co., 15.2:4
Indeco Sales, Inc. [*In re*], 20.2, 24.6:6
Indigital Solutions, LLC v. Mohammed, 24.6:6

Industrial Foundation of the South v. Texas Industrial Accident Board, 24.1

Cases Cited

Last Atlantis Capital, LLC v. AGS Specialist Partners

Ingersoll v. Farmland Foods, Inc., 2.5 Inhalation Plastics, Inc. v. Medex

Cardio-Pulmonary, Inc., 12.5

Innova Hosp. San Antonio, Ltd. P'ship v. Blue Cross & Blue Shield of Ga., Inc., 13.2:2

- In re (see name of party)
- IQ Holdings, Inc. v. Stewart Title Guar. Co., 15.3:11
- Irth Sols. v. Windstream Commc'ns LLC, 12.7

Isenberg v. Chase Bank USA, N.A., 13.2:4, 21.9

J

Jackson v. Equifax Info. Servs. LLC, 16.3:2 Jackson v. Haynes & Haynes, 15.2:11 Javeler Marine Servs. LLC v. Cross. 14.3 Jensen v. BMW of N. Am., LLC, 16.3, 16.3:2 J.H. Walker, Inc. [In re], 1.5:2, 15.3:11 Jimenez v. State, 18.3:7 J-M Mfg. Co. v. McDermott Will & Emery, 19.3:2 Johnson v. Ford Motor Co., 15.2:1 Johnson v. State, 18.3:4 Jones v. Beech Aircraft Corp., 20.6 Jones v. Bremen High School District 228, 2.4:2 Jones v. State, 18.2:22, 20.10 Jordan [In re], 9.2:1, 14.4:2 Joseph v. State, 18.2:9 JP Morgan Chase Bank, N.A. v. DataTreasury Corp., 13.2:2, 13.2:3 Junk v. Terminix Int'l Co., 16.3:2 Juster Acquisition Co., LLC v. North Hudson Sewerage Authority, 14.2:3 J.W. [In re], 20.7

K

KAIST IP US LLC v. Samsung Elecs. Co., Ltd., 13.2:1 Karrani v. JetBlue Airways Corp., 16.3 Keir v. Unumprovident Corp., 2.5 Keithley v. Home Store.com, Inc., 2.2 Keller v. Nat'l Farmers Union Prop. & Cas. Co., 20.2 Kellogg Brown & Root International Inc. v. Altanmia Commercial Marketing Co. W.L.L., 14.3 Kelly v. CSE Safeguard Insurance Co., 12.4:1 Kemper Lloyds Ins. Co. [In re], 24.6:6 Kidwiler v. Progressive Paloverde Ins. Co., 13.2:2 Kilmon v. Saulsbury Industries, Inc., 13.2:2 King v. Fidelity Nat. Bank of Baton Rouge, 13.2, 21.9 Kinnally v. Rogers Corp., 2.4:1 Kische USA LLC v. Simsek, 15.2:8 Kleen Products LLC v. Packaging Corp. of America, 6.8, 10.15:2, 14.2:3 Klezmer ex rel. Desyatnik v. Buynak, 14.2:6 Klipsch Group, Inc. v. ePRO E-Commerce Ltd., 1.10, 15.2:1, 15.2:5 Knight v. State, 18.2:23 Knoderer v. State Farm Lloyds, 15.3:11 Krause v. State, 25.8:6 Kronisch v. United States, 3.4 Kulzer [In re], 13.2, 21.9 Kyles v. Whitley, 25.8:3

L

Landry v. Air Line Pilots Ass'n, 13.2:3 Last Atlantis Capital, LLC v. AGS Specialist Partners, 14.2:1 Leidig v. Buzzfeed, Inc., 15.2:9 Lifesize, Inc. v. Chimene, 1.2 Lindquist v. City of Pasadena, Tex., 16.2:3 Lo [*Ex parte*], 25.8 Lokai Holdings LLC v. Twin Tiger USA LLC, 15.2:5, 15.2:10, 15.2:11 Lopez v. Don Herring Ltd., 13.2:2, 13.2:3 Lorraine v. Markel Am. Ins. Co., 6.6:1, 18.1, 18.2:7, 18.2:10, 18.2:13, 18.2:15, 18.2:17, 18.2:19, 18.2:20, 18.3:3, 18.3:5, 18.6 Louis Vuitton Malletier v. Texas International Partnership, 12.1 Lown v. State, 25.8

Luna Gaming-San Diego, LLC v. Dorsey & Whitney, LLP, 12.4:2

M

M. [In re], 14.4:1 Madden v. Wyeth, 23.2:2 Magellan Terminals Holdings, L.P. [In re], 20.2 Mailhoit v. Home Depot U.S.A., Inc., 20.2 Major Tours, Inc. v. Colorel, 2.3, 2.5, 14.2:3 Mancia v. Mayflower Textile Services Co., 6.8, 13.2:1, 13.2:2, 16.3, 23.2:3 Manuel v. State, 18.2:5, 18.2:7-18.2:9 Maracich v. Spears, 24.6:6 Marker v. Union Fidelity Life Ins. Co., 16.4:4, 16.5 Marten Transportation, Ltd. v. Plattform Advertising, Inc., 1.5:3, 1.6 Martin v. Allstate Ins. Co., 16.3:2 Martinez v. AA Foundries, Inc., 18.2:8 Martinez v. Midland Credit Management, Inc., 18.3:4

Mass Engineered Design, Inc. v. Ergotron, Inc., 16.4:4 Massimo v. State, 18.2:8, 18.3:5, 18.3:7, 25.8:7 McCarty v. State, 18.3:3 McKinney v. Nat'l Union Fire Ins. Co., 9.2:5 McKinney/Pearl Rest. Partners, L.P. v. Metro. Life Ins. Co., 9.3:2, 13.2:2, 16.4:4 McKissick v. State, 25.8:6 McLeod, Alexander, Powel & Apffel, P.C. v. Quarles, 13.2:2 McNickles v. Amaral, 20.10 Mercedes-Benz Emissions Litig. [In re], 23.2:2 Mercedes-Benz USA, LLC v. Carduco, Inc., 2.2, 15.3:11 Merck Eprova AG v. Gnosis S.P.A., 2.2, 14.2:6 Merial Ltd. v. Cipla Ltd., 23.2:1 Merrill v. Waffle House, Inc., 13.2:2 Methodist Primary Care Group [In re], 1.2, 9.2:1, 13.3:1 Miller v. State, 18.2:22, 18.3:5, 25.8:1 Miller v. York Rise Services Group, 16.3:1 Milton v. State, 18.3:1 Mims v. State, 18.3:6 Mims-Johnson v. Bechtel National, Inc., 16.4:1 Minpeco, S.A., v. Conticommodity Services, Inc., 23.2:2 Miranda v. State, 18.3:2 Mirmina v. Genpact LLC, 2.4:2 ML Healthcare Servs., LLC v. Publix Super Markets, Inc., 15.2:9 M.M.S. [In re], 18.3:4 Mohamed v. State, 20.10 Monitronics Int'l, Inc. v. iControl Networks, Inc., 13.2, 21.9

Monotype Corp. PLC v. Int'l Typeface Corp., 18.5:1 Montoya v. State, 18.2:9 Moody v. CSX Transportation, Inc., 15.2:5, 15.2:8, 15.2:11 Moore v. Publicis Groupe, 6.6:4, 6.8 Moore v. State, 18.2:23 Morgan Hill Concerned Parents Ass'n v. California Department of Education, 6.3 Mt. Hawley Insurance Co. v. Felman Production, Inc., 12.4:2 Mueller v. Swift, 15.2 Muro v. Target Corp., 2.5 Murray v. State, 18.2:6, 18.3:5 Musgrove v. State, 18.2:11

N

National Day Laborer Organizing Network v. U.S. Immigration and Customs Enforcement Agency, 8.9:2

National Lloyds Insurance Company [In re], 13.3:2

National Tank Co. v. Brotherton, 1.5:2, 15.3:3

Nat'l Health Res. Corp. v. TBF Fin., LLC, 18.3:4

Nat'l Lloyds Ins. Co. v. Lewis, 15.3:11

Nat'l Sec. Fire & Cas. Co. v. Lampson, 15.3:11

Netherlands Ins. Co. & American First Ins. Co. [*In re*], 24.7

Neutrino Development Corp. v. Sonosite, Inc., 14.3

Newberry v. Cty. of San Bernardino, 15.2:1

New Mexico Oncology & Hematology Consultants, Ltd. v. Presbyterian Healthcare Services, 2.4:2

Nguyen v. Excel Corp., 16.4:4

Nogle v. Beech Street Corp., 14.2:3 Norris v. State, 18.2 Nycomed U.S. Inc. v. Glenmark Generics, Ltd., 14.2:6

0

Olivarez v. GEO Group, Inc., 13.2:1 OOO Brunswick Rail Management v. Sultanov, 1.10 Oppenheimer Fund, Inc. v. Sanders, 14.2:1 Orbit One Communications, Inc. v. Numerex Corp., 2.4:1 Orchestratehr, Inc. v. Trombetta, 13.2:2, 13.2:3, 15.2 Organik Kimya, San ve Tic. A.S. v. Int'l Trade Comm'n, 15.2:11 Orillaneda v. French Culinary Inst., 16.3:2 ORIX USA Corp. v. Armentrout, 13.2:3 Ottoson v. SMBC Leasing & Fin., Inc., 15.2:1, 15.2:11 Overall v. S.W. Bell Yellow Pages, Inc., 9.2:4 Oxbow Carbon & Minerals LLC v. Union Pac. R.R. Co., 14.2:2

P

P.A. v. United Servs. Auto. Ass'n, 20.8
Pacific Coast Steel v. Leany, 12.1, 12.4:2, 12.4:3
Paparelli v. Prudential Ins. Co. of Am., 16.4:4
Parker v. Bill Melton Trucking, Inc., 13.2:2, 13.2:3
Parsons v. Jefferson-Pilot Corp., 13.2:2
Passlogix, Inc. v. 2FA Technology, LLC, 2.4:1
Patel v. Kuciemba, 18.3:4
Paxton v. City of Dallas, 24.6:2

Paxton v. City of Liberty, 24.6:2 Paxton v. Texas Health & Human Servs. Comm'n, 24.6:2 Payment Card Interchange Fee & Merchant Discount [In re], 14.4:1 Pension Committee v. Banc of America Securities, LLC, 2.4:1, 3.8 People v. Johnson, 18.3:7 People v. Pierre, 18.2:6 Perfect 10, Inc. v. Cybernet Ventures, Inc., 18.3:7 Perry v. State, 25.8:6 Peskoff v. Faber, 2.4:2, 14.2:3 Peter Kiewit Sons', Inc. v. Wall St. Equity Grp., Inc., 19.2:2 Petroleum Solutions, Inc. v. Head, 15.3:9, 15.3:11 Phillip M. Adams & Assoc., LLC v. Dell, Inc., 19.2:5 Phillip M. Adams & Assoc., LLC v. Winbond Elecs. Corp., 19.2:5 Phoenix Four, Inc. v. Strategic Resources Corp., 19.2:2, 19.2:5 Pilgrim's Pride Corp. v. Mansfield, 15.3:11 Pinnacle Engineering, Inc. [In re], 14.4:2, 24.6:5 Pipefitters Local No. 636 Pension Fund v. Mercer Human Resource Consulting, Inc., 14.2:3 Playboy Enterprises, Inc. v. Welles, 14.1 Porter v. State, 25.8 Positive Black Talk Inc. v. Cash Money Records, Inc., 13.2, 21.9 Powell v. Hocker, 25.8:6 PPM Fin., Inc. v. Norandal, USA, Inc., 16.4:2 Price v. State, 18.2 Progressive Cas. Ins. Co. v. Delaney, 10.1, 10.13, 10.15, 10.16 Prokosch v. Catalina Lighting, Inc., 16.2:1, 16.4:1

Pugh v. State, 18.5:2

Pulsecard, Inc. v. Discover Card Servs., Inc., 13.2:2

Q

QBE Ins. Corp. v. Jorda Enters., Inc., 16.2:1
Qualcomm Inc. v. Broadcom Corp., 8.9:2
Quantlab Techs. Ltd. (BVI) v. Godlevsky, 15.2:1

R

Rabbani v. State, 18.3:3 Race Tires America, Inc. v. Hoosier Racing Tire Corp., 14.3 Rafeedie v. L.L.C., Inc., 24.6:3 Rajala v. McGuire Woods, LLP, 12.7 Rambus, Inc. v. Infineon Techs, AG, 18.2:8 RealPage, Inc. v. Enter. Risk Control, LLC, 15.2:11 Reavis v. State, 18.2:18 Reed v. Bennett, 16.4:1 Reed Elsevier, Inc. v. Muchnick, 13.2, 21.9 Regan-Touhy v. Walgreen Co., 13.2:2 Reilly v. Nat'l Markets Grp. Inc., 16.2:4 Relion, Inc. v. Hydra Fuel Cell Corp., 12.4:2 Rene v. State, 18.2:12, 20.7 Resolution Trust Corp. v. S. Union Co., Inc., 16.4:3, 16.4:4 Rezulin Prods. Liab. Litig. [In re], 24.7 Rhoads Indus., Inc. v. Bldg. Materials Corp. of America, 12.1, 12.4:2, 12.4:3 Richmond v. SW Closeouts, Inc., 13.2:2 Rife v. Oklahoma Dep't of Pub. Safety, 15.2:11

Cases Cited

Riley v. Walgreen Co., 24.7 Rimkus Consulting Group, Inc. v. Cammarata, 1.5:1 Rios v. State, 18.2:22 Rio Tinto PLC v. Vale S.A., 8.9:2, 10.11, 10.13, 10.15, 10.15:1, 10.16 Rivastigmine Patent Litigation [In re]. 23.5:2 Rivera v. United States, 13.2:2 R.K. v. Ramirez, 24.6:1 Robinson v. Harkins & Co., 18.3:2 Robinson v. Jones Lang Lasalle Americas, Inc., 20.2 Robinson v. State, 18.3:1 Robroy Indus.-Tex., LLC v. Thomas & Betts Corp., 13.2:1, 13.2:2 Rodriguez v. Pataki, 16.4:2 Rodriguez-Torres v. Government Development Bank of Puerto Rico. 6.7 Rogers v. State, 25.8:6 Romero v. Allstate Insurance Co., 6.6:2, 6.8 Rowe Entertainment, Inc. v. William Morris Agency, Inc., 21.3 Royal Park Investments SA/NV v. HSBC Bank USA, N.A., 24.8 R.R. Comm'n v. S. Pac. Co., 18.1 Ruff v. State, 18.2:21 R.Z. v. Tex. Dep't of Family & Protective Servs., 18.2:12 S Sabatino v. Curtiss Nat'l Bank, 18.3:4 Sacks v. Zimmerman, 24.6:1 Safeco Insurance Co. of America v. Burr, 15.3:7 Salt River Project Agric. Improvement & Power Dist. v. Trench France

SAS, 24.8

Samsung Electronics Am., Inc. v. Chung, 13.2:1, 13.2:3 Sanders Oil & Gas, Ltd. v. Big Lake Kay Construction, Inc., 1.5:2 Satterfield v. Chipotle Mexican Grill, Inc., 15.2:1 Savage v. State, 25.8:6 Scarbrough v. Purser, 15.3:11 Schlafly v. Caro-Kann Corp., 13.2:1 Schmalz v. Vill. of N. Riverside, 15.2:8 Schreiber v. Schreiber, 22,11:3 Schultz v. Commission for Lawyer Discipline, 25.8:3 Schwimmer v. United States, 25.2 Scofield v. Parlin & Orendorff Co., 18.2:5 Sea-Land Serv., Inc. v. Lozen Int'l. 18.2:16 S.E.C. v. Brady, 13.2:2 S.E.C. v. Mazzo, 13.2:2 Securities & Exchange Commission v. Stanford International Bank Ltd., 23.2:2 Segovia v State, 18.1 Semtek Int'l, Inc. v. Merkuriy Ltd., 13.2, 21.9 Sennett v. State, 18.2:8 Seoul Semiconductor Co. Ltd. v. Nichia Corp., 23.2:2 Seroquel Products Liability Litigation [*In re*], 6.6:2 Service Lloyds Insurance Co. v. Martin. 1.6:2 Sewell v. D'Alessandro & Woodyard, Inc., 13.2:2 Shaffer v. State, 18.3:4 Shamoun & Norman, LLP v. Hill, 1.5:2, 15.3:11 Shanklin v. Columbia Management Advisors, L.L.C., 24.6:6 Shea v. State, 18.2:8

829

Shenwick v. Twitter. Inc., 2.5 Shipman [In re], 9.2:1, 13.3:1, 24.6:5 Sidney I. v. Focused Retail Property I. LLC, 12.4:2, 12.4:3 Silvestri v. General Motors Corp., 1.5, 1.6:1 Simmons [In re], 25.8 Simon v. City of New York, 15.2:8 Simone v. VSL Pharm., Inc., 15.2 Simpson v. State, 18.2:21 Sinclair v. Cambria Cty., 15.2:8, 15.2:10 Sinclair Wyo. Ref. Co. v. A&B Builders, Ltd., 16.3 Ski Train Fire of Nov. 11, 2000 Kaprun Austria [In re], 16.4:3 Small v. Univ. Med. Ctr., 15.2:5, 15.2:9 SmartPhone Technologies LLC. v. Apple, Inc., 6.5 Smith v. Our Lady of the Lake Hosp., Inc., 13.2:1 Smith v. Williams, 15.3:11 Snider v. Danfoss, LLC, 15.2:4, 15.2:8, 15.2:10 Societe Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa, 23.2:2. 23.7:1 Source Network Sales & Marketing. LLC v. Jiangsu Mega Motor Company, 13.2:2 SprayFoamPolymers.com, LLC v. Luciano, 20.6 Sprint Communications Co., L.P. v. Comcast Cable Communications, LLC, 13.2:2 St. Angelo v. State, 18.2:8 Starbucks Corp. v. ADT Sec. Servs., Inc., 16.3:1 Starlight Int'l Inc. v. Herlihy, 16.2:1, 16.4:1 State [In re], 25.8:4 State v. Boothby, 18.2:8

State v. Burns, 18.2:12 State v. Cheever, 18.2:8 State v. Dunn, 18.2:16, 18.3:7 State v. Eleck, 18.2:12 State v. Hall, 18.2:16, 18.3:7 State v. Hardy, 24.6:1 State v. Huse, 24.6:1 State v. Jewell, 24.6:1 State v. Martinez, 24.6:1 State v. Robinson, 18.2:8 State v. Sayles, 18.5:2 State v. Swinton, 18.2:20 State Auto. Mut. Ins. Co. v. Freehold Mgmt., Inc., 13.2:1, 13.2:2 State ex rel. Skurka [In re], 25.8:2 State Farm Lloyds [In re], 5.9:1, 6.3, 9.2:1, 9.2:3, 9.2:6, 13.3:1, 14.4:3 State of Texas [In re], 25.8 St. Clair v. Johnny's Oyster & Shrimp, Inc., 18.1, 18.5:4 Steenbergen v. Ford Motor Co., 9.2:4 Stevenson v. State, 18.3:5 Steves & Sons, Inc. v. JELD-WEN, Inc., 15.2:6 St. Luke's Cataract & Laser Inst., P.A. v. Sanderson, 18.2:11 Strahan v. Strahan, 18.3:4 Strauss v. Credit Lyonnais, S.A., 23.2:2 Structural Metals, Inc. v. S&C Electric Co., 14.3 Surplus Source Group, LLC v. Mid America Engine, Inc., 14.2:4

T

Tadayon v. Greyhound Lines, Inc., 6.8
Takata Airbag Prod. Liab. Litig. [*In re*], 24.7
Taniguchi v. Kan Pacific Saipan, Ltd., 14.3
Taylor v. State, 25.8:6

Team Express Distributing, LLC v. Junction Solutions, Inc., 13.2:2

- Telesis/Parkwood Ret. I, Ltd. v. Anderson, 15.3:11
- Telewizja Polska USA, Inc. v. Echostar Satellite Corp., 18.3:7
- Terra Int'l [In re], 13.2:3
- Texas v. City of Frisco, 6.8

Texas State Board of Chiropractic Examiners v. Abbott, 24.6:2

Texas State Employees Union v. Tex. Dept. of Mental Health & Mental Retardation, 24.1

Tex. Black Iron, Inc. v. Arawak Energy Int'l Ltd., 18.2:3

- Tex. Gen. Land Office v. Porretto, 9.2:5
- Thierry v. State, 18.2:21

Third Pentacle, LLC v. Interactive Life Forms, LLC, 13.2:2

Thorncreek Apartments III, LLC v. Village of Park Forest, 12.4:1, 12.4:2

Tienda v. State, 18.2, 20.7, 25.8:7

Timberlake v. Synthes Spine Co., L.P., 24.7

TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo, 15.2:11

Tompkins v. Detroit Metro. Airport, 20.2

Toussie v. Allstate Insurance Co., 1.10

Toyota Motor Sales, U.S.A., Inc. [*In re*], 13.3:1

Trainer v. Cont'l Carbonic Prod., Inc., 15.2:4

- Trevino v. Ortega, 1.5:2, 15.3:4, 15.3:5, 15.3:8
- T-Rex Prop. AB v. JCDecaux N. Am., Inc., 14.3
- Triumph Aerostructures LLC v. Comau, Inc., 23.2:2

Trueposition, Inc. v. LM Ericsson Telephone Co., 23.3:2 Tsanacas v. Amazon.com, Inc., 13.2:2
T.T. [*In re*], 18.3:7
Turner v. Hudson Transit Lines, Inc., 3.4, 7.2:2
Turner v. Nationstar Mortg. LLC, 13.2:2
Turner v. Resort Condominium International, LLC, 2.5
Twentieth Century Fox Film Corp. v. Marvel Enters., Inc., 16.4:3
246 Sears Rd. Realty Corp. v. Exxon

Mobil Corp., 16.3:3

\$201,100.00 U.S. Currency v. State, 18.2:23

2M Asset Management, LLC v. Netmass Inc., 23.5:2

U

Ukwuachu v. State, 18.3:6 Union Energy, Inc. [In re], 24.6:6 United Medical Supply Co., Inc. v. United States, 2.5 United States [In re], 13.2:2 United States v. Abrams, 25.5 United States v. Aluminum Co. of America, 23.2:1 United States v. Ballesteros, 20.10 United States v. Barlow, 18.2:14 United States v. Black, 25.2 United States v. Briggs, 25.5 United States v. Cadden, 25.3 United States v. Carter, 25.5 United States v. Cross, 25.4 United States v. Fadayini, 18.2:18 United States v. Fattah, 25.3 United States v. Fumo, 19.4:4 United States v. Garrett, 13.2:3 United States v. Goichman, 18.2 United States v. Jackson, 18.2:11, 18.3:1 United States v. Jean, 25.5 United States v. Johnson, 18.3:7

United States v. Kassimu, 18.2:16 United States v. Khorozian, 18.3:7 United States v. Ledford, 18.3:3 United States v. Meienberg, 18.2:16 United States v. Mills, 18.5:1 United States v. Mitchell, 25.7:3 United States v. Nat'l Steel Corp., 13.2:2 United States v. O'Keefe, 8.9:2, 25.3 United States v. Regents of New Mexico State Univ., 15.2:1 United States v. Reyna, 25.5 United States v. Robinson, 12.1 United States v. Rollins, 18.3:7 United States v. Rubin/Chambers, 25.6 United States v. Safavian, 5.11, 18.2, 18.3:7 United States v. Salyer, 25.6 United States v. Schweitzer, 18.3:6 United States v. Shaffer Equipment Co., 1.5 United States v. Siddiqui, 18.2:8 United States v. Simpson, 18.2:14 United States v. Skilling, 25.6 United States v. Soliman, 25.3 United States v. Tank, 18.2:14 United States v. Trinity Industries, Inc., 1.2, 2.2 United States v. Warshak, 25.6 United States v. Weinstein, 18.2:5 United States v. Wolfson, 18.2:5 United States ex rel. Carter v. Bridgepoint Educ., Inc., 9.3:5, 14.2:4 United States ex rel. Scutellaro v. Capitol Supply, Inc., 15.2:1 United States Sec. & Exch. Comm'n v. Commonwealth Advisors, Inc., 13.2:2

Universal Serv. Fund Tel. Billing Practices Litig. [In re], 12.3

V

Vailes v. Rapides Par. Sch. Bd., 13.2:2 Valentin v. Bank of New York Mellon Corp., 12.4:2, 12.4:3 Valeo Elec. Sys., Inc. v. Cleveland Die & Mfg. Co., 9.3:2 Vallejo v. Amgen, Inc., 13.2:3 Vann v. Mattress Firm, 24.7 Varkonvi v. State, 18.2:5 Vasquez v. Conquest Completion Services, LLC, 13.2:2 Vaughan [In re], 24.6:3 Vee Vinhnee [In re], 18.2:16 VERP Inv., LLC [In re], 24.6:5 Viagra (Sildenafil Citrate) Prod. Liab. Litig. [In re], 10.15, 10.15:1, 10.15:2 Victor Stanley, Inc. v. Creative Pipe, Inc., 1.5, 12.1, 12.3, 12.4:3 Vital v. Nat'l Oilwell Varco, L.P., 14.3 Vital v. Varco, 14.3 Volkswagen AG v. Valdez, 24.8 VOOM HD Holdings, LLC v. EchoStar Satellite L.L.C., 14.1

W

Wackenhut Corp. v. Gutierrez, 15.3:11
Wal-Mart Stores v. Johnson, 7.2:2, 15.3:3
Wal-Mart Stores, Inc. v. Texas Alcoholic Beverage Commission, 13.2:2

Washington v. M. Hanna Const. Inc., 13.2:3

Washington v. Wal-Mart Louisiana LLC, 15.2:4, 15.2:11

Waste Management of Texas, Inc. [*In* re], 9.2:2, 14.4:1

Waterman Steamship Corp. v. Ruiz, 20.6

Cases Cited

Waters v. Lincoln Gen'l Ins. Co., 13.2, 21.9 Watkins v. HireRight, Inc., 16.3:1 Waymo LLC v. Uber Technologies, Inc., 1.11, 15.2:11 Weekley Homes, L.P. [In re], 5.8, 6.1, 8.9:1, 9.2:1, 13.3:1, 14.4, 14.4:1, 14.4:2, 21.4, 22.6, 24.6:5 Whalen v. Roe, 24.1 W Holding Co., Inc. v. Chartis Insurance Co. of Puerto Rico, 14.2:3 Wilkerson v. RSL Funding, L.L.C., 20.6 Williams v. Angie's List, Inc., 1.2 Williams v. City of Dallas, 13.2, 21.9 Williams v. Dist. of Columbia, 12.4:2, 12.4:3 Williams v. Sprint/United Management Co., 6.3 Williams Farms Produce Sales, Inc. v. R&G Produce Co., 18.2:2, 18.2:6 Winfield v. City of New York, 10.13, 10.15, 10.15:1, 12.6, 16.3:1, 16.4:1 Wiwa v. Royal Dutch Petroleum Co., 13.2.21.9 Wm. T. Thompson Co. v. General Nutrition Corp., 15.3:4 World Trade Centers Ass'n v. Port Auth. of New York & New Jersey, 15.2:3

W. Power, Inc. v. TransAmerican Power Prod., Inc., 15.2:5
Wright [*In re*], 19.3:3
Wright v. Nat'l Interstate Ins. Co.,

15.2:11

Wright v. Weaver, 24.6:6

WWP, Inc. v. Wounded Warriors Family Support, Inc., 14.1

X

Xpel Techs. Corp. v. American Filter Film Distributors, 22.12Xterra Construction, LLC [*In re*], 1.5:2

Y

Youkers v. State, 20.8

Z

Zamora v. Stellar Mgmt. Grp., Inc., 15.2 Zaratti v. State, 25.8:6

Zimmerman v. Weis Markets, Inc., 20.2

Zippo Mfg. Co. v. Zippo Dot Com, Inc., 20.6

Zubulake v. UBS Warburg LLC, 1.5:1, 2.2, 2.4:1, 3.4, 5.2, 8.2:3, 13.2:1, 14.2:3, 14.2:4, 21.4, 23.2



Subject Index

[References are to sections in the text.]

A

Accessible vs. inaccessible formats, 14.2:3 Accessing data, general precautions, 4.10 Acquisition protocol, sample, 22.12 Admissibility of electronic information. See also Authentication of electronic information generally, 18.1, 18.5 best-evidence rule, 18.3:1 business records, 18.2:15 checklist, 18.1 depositions, 16.2:3 e-mail, 5.11 governing rules, 18.1 hearsay issues (see Hearsay; Hearsay exceptions; Nonhearsay) historically, 18.1 social media content, 20.2 unfair prejudice, 18.4

examples, 18.2:1 Facebook messages, 18.2:12, 20.7, 20.8, 20.9, 20.10 judicial discretion, 18.2 methods, 18.2:1 native production, 9.5 nonparty discovery, 21.2:3, 21.2:4 photographs, 18.2:17 procedure, 18,2:24 self-authentication, 18.2:2, 18.2:5, 18.2:6, 18.2:7 showing required, 18.2 social media content, 18.2:12, 20.7 stored data, 18.2:14, 18.2:16 text messages, 18.2:9 videos, 18.2:17 voice mails, 18.2:22, 18.2:23 website postings, 18.2:10

B

Backup practices, 7.3:5

Backup tapes duty to preserve, 6.4 inaccessibility, 14.2:3

Bank account information, 24.6:6

Best-evidence rule, 18.3:1

Binary system, 4.2:2

Bits, defined, 4.2:3

Boolean searches, 8.6:5

Bring-your-own-device policies, 3.2:4

Business records authentication, 18.2:5 hearsay exception, 18.3:4, 18.3:5

Bytes, defined, 4.2:4

Admissions by party-opponent, 18.3:5

Alternative source locations, 26.1:3

American Standard Code for Information Exchange (ASCII), 4.2:5

Apple devices, 7.3:1

Attorney competence, 5.2, 19.2:2

Authentication of electronic information generally, 18.2 audio recordings, 18.2:22 business records, 18.2:15, 18.2:16 chat room content, 18.2:13, 18.2:14 digital photographs, 18.2:17, 18.2:18,

18.2:19, 18.2:20, 18.2:21 e-mail, 18.2:7, 18.2:8

Essentials of E-Discovery

С

Candor, attorney's duty, 19.2:4

Cell phones, 24.6:6

Central processing unit (CPU), 4.7

Chat room content, authentication, 18.2:13

Checklists

admissibility issues, 18.1 criminal cases, ESI protocol, 25.3 cross-border issues, 23.7, 23.7:1, 23.7:2, 23.7:3, 23.7:4 meet and confer, 5.8, 6.7

Child pornography cases, 25.7:3, 25.8, 25.8:4, 25.8:5, 25.8:6

Claims and defense assessment, 2.4:2

Class actions, cost shifting, 14.2:5

Clawback agreements, 6.2:4, 6.5, 12.2, 12.7

Cloud computing

benefits, 19.3:1 confidentiality issues, 19.3:1 ethics issues, 19.2:5, 19.3:1 international issues, 23.5:1, 23.7:4 servers, 4.8:1, 5.7

Clustering, 8.8:1

Collaborative work sites, 5.1

Collection of electronically stored information

generally, 7.4, 7.5 cautions, 7.5 early start, 7.1 full replication, 7.4:1 Internet collections, 7.4:4 least intrusive means, 14.4:2 methods generally, 7.4 on-site collection, 7.4:2 practical tips, 7.5 remote collection kits, 7.4:3 self-collection by client, 7.4:5 targeted collection, 7.4:1 tools, 7.4

Color detection, 11.16:5

Complex keyword search, 8.6:5

Compound document, 11.8:3

Computer forensics

generally, 22.1 acquisition protocol, sample, 22.12 cost, 22.16 defined, 22.1 devices at issue, 22.16 duplication vs. examination, 22.11:2 electronic discovery distinguished, 22.2 examination protocol, 22.11, 22.13 experts, 22.7 ghost images of drives, 22.16 hashing, 4.3:8 intrusiveness, 22.16 limitations, 22.5 neutral examiner, selection, 22.3, 22.6 privacy, balancing, 22.6, 22.16 procedure for compelling use, 22.6 servers, 22.16 status quo, preservation, 22.16 supervision, 22.11:2 use, 22.3, 22.4

Computer terminology

American Standard Code for Information Exchange (ASCII), 4.2:5 binary system, 4.2:2 bits, 4.2:3 bytes, 4.2:4 central processing unit (CPU), 4.7 digital data, 4.2 graphics processor unit (GPU), 4.7 network adapter, 4.7 random access memory (RAM), 4.7 servers (*see* Servers) sound card, 4.7

Computer usage policies bring-your-own-device policies, 3.2:4

company data, downloading, 3.2:8

Subject Index

Criminal cases

confidentiality, 3.2:7 contents, 3.2:2, 3.2:6 e-mail (*see* E-mail) explicit use policies, 3.2:9 Internet use, 3.2:2 password policies, 1.5:5 personal devices, 3.2:4 personal documents, 3.2:4 privacy, 3.2:14 retention policies (*see* Document retention policies (DRPs)) terminated employees, 3.2:11 virtual private networks, 3.2:13 white-listing, 3.2:12

Concept searching, 8.8:2

Concordance index, 11.14

Confidentiality

agreements, 24.7 attorney technology practices, 19.2:2, 19.3:1 cloud computing, 19.3:1 company policies, 3.2 ethics issues, 19.2:2, 19.3:1 protective orders, 24.2:2

Confidentiality agreements, 24.7

Containers, 11.8:4, 11.8:5, 26.1:5

Content, 11.16:6, 26.1:5

Control, 26.1:10

Cooperation, importance, 5.8, 6.8, 19.2:1

Coordinating discovery attorney, 25.3

Corporate depositions. See Depositions

Cost shifting. *See also* Costs; Undue burden or cost generally, 14.5 American rule, 14.2:1 class actions, 14.2:5 cost recovery in federal court, 14.3 court's discretion, 14.2:2 factors, 14.2:3, 14.2:4 fault of requesting party, 14.2:3 federal court, 14.2:1, 14.2:2, 14.2:3, 21.9:4 inaccessibility of data as prerequisite, 14.2:3 one-sided discovery, 14.2:5 prevailing party, recovery of costs, 14.3 proportionality, 14.2:4 sanction, 14.2:6 Texas state court, 14.4 trends, 14.1, 14.2:3, 14.2:4 *Zubulake* case, 14.2:3

Costs. See also Cost shifting; Undue burden or cost criminal cases, federal, 25.7:1 forensic examinations, 22.16 nonparty discovery, 21.2:4, 21.3, 21.9:4 prevailing party, recovery by, 14.3 shifting (see Cost shifting)

Criminal cases

agreements regarding electronically stored information, topics, 25.8:6 best practices (see ESI protocol, criminal cases) child pornography cases, 25.7:3, 25.8, 25.8:4, 25.8:6 contraband, 25.7:3, 25.8:6 costs, 25.7:1 defense access to electronically stored information, arguments supporting, 25.8:7 duty to preserve, 1.5:3 ESI Protocol (see ESI protocol, criminal cases) exculpatory information, disclosure, 25.6 federal cases, 25.7:1, 25.7:2, 25.7:3, 25.7:4. 25.7:5 incarcerated clients, 25.7:5 law enforcement practices, 25.8 metadata, 25.7:4 non-releasable information, 25.7:3, 25.8:5 prosecutor practices, state, 25.8, 25.8:1 protected information, 25.7:2 social media evidence, 20.10 statutory history, 25.8:1 Texas state cases, 25.8

Cross-border issues

Cross-border issues binding corporate rules, 23.4:4 blocking statutes, 23.3:2 challenges generally, 23.1 checklist, 23.7:1 cloud computing, 23.5:1, 23.7:4 consent, 23.4:5 cooperation, 23.4:1 corporate rules, 23.4:4 data privacy regulations, 23.3:1, 23.3:2, 24.8 Federal Rules of Civil Procedure, 23.2:3 foreign laws limited disclosure, generally, 23.3 Hague Convention, 23.2:2 in-country review, 23.4:7 minimizing conflicts, 23.6 mutual legal assistance treaties, 23.2:2 national security concerns, 23.3:3, 23.7:2 personal jurisdiction, 23.2:1, 23.7:1 practical tips, 23.6 privilege issues, 23.5:2, 23.7:3 protective orders, 23.4:2 Safe Harbor Framework (European Union), 23.4:6 sensitive information, 23.2:2, 23.7:3 solutions, 23.4, 23.4:1, 23.4:2, 23.4:3, 23.4:4, 23.4:5, 23.4:6, 23.4:7 standardized contract clauses, 23.4:5 state secrets, 23.3:3, 23.4:2 work product issues, 23.4:5, 23.7:2

Cryptographic hashing, 11.15:2

Culling electronically stored information generally, 8.1 benefits, 8.7 datasets, 11.15 deduplication, 8.6:3 defined, 8.3:1, 8.3:2 place in e-discovery process, 8.2:3 purpose, 8.3:1, 8.3:2, 8.4:1, 8.4:2, 8.4:3 system file filtering, 8.6:2

Custodian interviews, 7.3, 7.3:1, 7.3:2, 7.3:3, 7.3:4, 7.3:5

Custody, 26.1:10

D

Data, 26.1:9 Databases, 9.7, 11.14:1 Data compression, 11.4 Data extraction, 11.7 Data maps, 7.2:4, 17.4:4 Data sampling, 6.6:3 Data Security, 9.5 Data sets, 11.15 **Data storage practices**, 7.3:5 Decryption, 11.16:3 Deduplication, 11.15:3 Definitions American Standard Code for Information Exchange (ASCII), 4.2:5 binary system, 4.2:2 bits, 4.2:3 bytes, 4.2:4 central processing unit (CPU), 4.7 computer forensics, 22.1 culling, 8.3:2 digital data, 4.2 document retention policy (DRP), 3.3 filtering, 8.3:2 forensics, 22.1 graphics processor unit (GPU), 4.7 hearsay, 18.3:2, 18.3:5 inadvertent disclosure, 12.4:1 metadata, 5.5 mobile device, 26.2:1, 26.2:2, 26.2:3 native file, 6.3 network adapter, 4.7 portable document format, 6.3 predictive coding, 10.1 privilege, 12.1 random access memory (RAM), 4.7 reviewing, 8.11:1 searching, 8.3:1
server, 4.8 sound card, 4.7 tagged image file format, 6.3 work product protection, 8.10:2, 12.1 Depositions generally, 16.1, 16.2:1, 16.2:2, 16.2:3. 16.2:4 governing rules, 16.1, 16.2:1, 16.2:2, 16.2:3, 16.2:4 limits, 16.4:1 multiple witnesses, 16.4:2 nonemployee vendors as witnesses, 16.4:2 nonparties, production of electronically stored information, 21.2:3 notice, 16.2:1, 16.4:1, 16.5, 21.2:3, 21.2:4 objections, 16.4:4 perpetuating testimony, 21.5, 21.5:1, 21.10, 21.10:1 preparation of witness, 16.2:1, 16.4:2 protective orders, 16.3:3 purpose, 16.1 reasonably available information, 16.4:3 relevance challenges, 16.3:2 representative status of deponent, 16.4:4 sanctions, 16.5 scope of notice, 16.4:1 selection of witness, 16.4:2 technical knowledge of witness, 16.4:2 use at trial, 16.2:3 use in mediation, 17.3 witness preparation, 16.1, 16.4:3 witness selection, 16.1, 16.4:2

De-NISTing, 11.15:1

Device collection, 26.1:7

Device data, 26.1:4, 26.1:6

Device forensics, 26.1:1

Device inventory, 4.10, 14.1

Digital data, defined, 4.2

Digital photographs, authentication, 18.2:7, 18.2:18, 18.2:19, 18.2:20, 18.2:21 Diligence, attorney's duty, 19.2:5

Discovery plan, 3.6, 6.2:4

Document filters, 11.7

Document retention policies (DRPs) generally, 1.4, 3.1, 3.2:1–3.2:14, 3.2 audits, 3.3 benefits, 3.3, 7.2:2 contents, 3.3 defined, 7.2:2 former employees, 7.2:3 importance, 3.8 purpose, 3.2 suspension, 2.4:2

Document review. See Reviewing electronically stored information

Duty to preserve

agreement of parties, 6.4 backup tapes, 6.4 breach, 15.3:2 counsel's duty, 2.4:2 demand letter, effect, 1.5:3 disaster recovery records, 7.6 effective date, 3.3 federal law, 1.6:1 format, 1.9 good faith, effect, 1.8 jury instructions, 1.1 litigation potential as trigger (see Litigation hold) metadata, 1.9 overview, 1.1, 1.13 parties having duty, 1.2, 1.5:2 proportionality, effect, 1.8 reasonable efforts, 1.8, 1.9 relevant information, defining, 1.5:1, 1.5:2, 1.5:3 routine destruction of data (see Document retention policies (DRPs)) steps of compliance, 1.4 timeliness, 26.1:8 third-party-held documents, 1.12

E

E-commerce, jurisdiction issues, 20.6

E-mail admissibility, 5.11 appearance, 5.5 authentication, 18.2:7 delivery, 5.6 forgery, 5.11 "from" field, 5.5 history, 5.3 HTTP systems, 5.6 identification codes, 5.5 IMAP systems, 5.6 importance, 5.9:1 IP address, 5.5 locating, 5.9:2 MAPI systems, 5.6 metadata, 5.5, 5.10 mining, 5.10 overview, 5.1 pervasiveness, 5.4 policies generally, 3.2:5 POP3 systems, 5.6 protocols, 5.5 reliability, assessing, 5.11 reviewing, 5.10 servers, 5.7 target information by type of case, 5.9:1 text-based nature, 5.5 time of message, 5.5

Embedded data, 11.8

E-mediation. See Mediation of disputes

E-neutrals. See Special masters

Entropy testing, 11.16:2

Entry on property, 21.7

ESI protocol, criminal cases generally, 25.1 applicability, 25.3 coordinating discovery attorney, multiple defendant cases, 25.3 discovery disputes, 25.3 meet-and-confer provisions, 25.3 nonbinding status, 25.1 organization, 25.3 overview, 25.1 production of electronically stored information, 25.3 purpose, 25.3 structure, 25.3

Ethics issues

generally, 19.5 attorney competence, 5.2, 19.2:2 candor, 19.2:4 cloud computing, 19.3:1 cooperation, 19.2:1 diligence, 19.2:5 document review, outsourcing, 19.3:2 metadata, 18.3:5, 19.3:4 outsourcing, 19.3:2 social media, 19.4, 19.4:1, 19.4:2, 19.4:3, 19.4:4 zealous representation, 19.2:1

Exceptions reporting, 11.10

Excited utterance, 18.3:3

Experts forensics, 22.7 predictive coding, 10.2

Extensions, 11.16:4

Extracted text, 11.11

F

Facebook. See Social media and networking sites

Family tracking, 11.9

Federal Rule of Evidence 502, 12.4

Federal Rules of Civil Procedure applicable rules, 6.7

File extensions, 11.3:2

File matching, 4.4

File signatures, 11.3:2

File structure, 11.3:2

Filtering electronically stored information. See also Culling electronically stored information date-based, 8.3:1, 8.6:4 defined, 8.3:1, 8.3:2 metadata, using, 8.6:4

Financial information and privacy issues, 24.6:3

Flash drives, 4.3:6

Foreign countries. See Cross-border issues

Foreign language detection, 11.16:1

Forensics. See Computer forensics

Form of production

generally, 6.3 determining format, 9.3:3 load files, 9.4 metadata, 6.3 native format, 9.3:4, 9.4:1, 9.4:3, 9.5 portable document format (PDF), 6.3 reasonable usability, 9.3:4, 9.3:5 searchability, 6.3 tagged image file format (TIFF), 6.3

Former employees

computer usage policies, 3.2:11 document retention policies, 7.2:2

Freedom of Information Act requests, 8.9:2

Graphics processor unit (GPU), 4.7

H

Hague Convention, 23.2:2

Hard drives, 4.3:5

Hashing, 11.15:2

Health Insurance Portability and Accountability Act (HIPAA), 24.6:1

Hearsay. See also Hearsay exceptions; Nonhearsay defined, 18.3:2, 18.3:5 general rule, 18.3:2

Hearsay exceptions generally, 18.3:2 business records, 18.3:4 commercial publications, 18.3:4 excited utterance, 18.3:3 market reports, 18.3:4 present sense impression, 18.3:3 rationale, 18.3:3 recollection recorded, 18.3:4 regularly conducted activity, records, 18.3:4 reliable documents generally, 18.3:4 then-existing condition, 18.3:3 unreflective statements generally, 18.3:3

Hit report, 8.5:4

HTTP e-mail systems, 5.6

I

Imaging, 26.1:2

Inaccessible information, 14.2:3

Inadvertent disclosure generally, 6.2:4, 6.5 burden of proof, 12.4:1 clawback agreements, 6.2:4, 6.5, 12.2, 12.7 defined, 12.4:1 extent, 12.4:2

G

Ghost images of hard drives, 22.16

Google apps, 5.7

Governing rules federal, 6.7 Texas, 25.8:1

Inadvertent disclosure

federal rule generally, 12.3, 12.8 order protecting privilege, 12.5, 12.6 prevention, 12.4:2 prompt action required, 12.4:2 reasonable steps to prevent, 12.4:2 rectification, 12.4:3 sneak peek agreements, 12.7 Texas rules, 12.2, 12.8 waiver resulting (*see* Waiver of privilege by inadvertent disclosure)

Indexing, 11.14

Instant messages, 7.2:7

Insurance policyholder information, 24.6:6

International discovery. See Cross-border issues

IT interviews, 7.2:1

J

Jump drives, 4.3:6

Jurisdiction issues e-commerce, 20.6 foreign entities, 23.2:1, 23.7:1 United States entities, 20.6

Jurors' Internet searches, 19.4:4

K

Keyword search

generally, 6.6:2, 8.3, 8.6:5 Boolean, 8.6:5 complex, 8.6:5 simple, 8.6:5 stemming, 8.6:5 wildcard, 8.6:5

L

Litigation hold. See also Litigation-hold memorandum best practices, 2.2 definition, 2.1 document retention, suspension, 2.4:2 failure, 2.2 Google Apps, 5.7 importance, 2.2 lifting, 2.6 Microsoft Exchange, 5.7 obstacles, 2.2 personal technology devices, applicability, 3.2:8 preservation, 2.2, 3.4 response, 3.8 routine document destruction, suspension, 2.4:2 scope, 2.5, 3.4 spoliation, 2.2 tracking and verification, 2.4:2 writing, 2.4:1

Litigation-hold memorandum

acknowledgment of receipt, 2.4:2 contents generally, 2.4:2 discoverability, 2.5 document identification, 2.4:2 drafting, 2.3 overview, 2.2 privilege, 2.5 purpose, 2.4:2 samples, 2.7 tailoring, necessity, 2.3 work product protection, 2.5

Litigation trigger of duty to preserve. See also Litigation hold; Litigation-hold

memorandum generally, 1.5, 1.9 criminal cases, 1.5:3 duration, 1.5 individuals covered, 1.5 scope, 1.6, 1.7 timing, 1.5

Multipurpose Internet Mail Extensions (MIME)

Load files, 6.3, 9.4:2

Local servers, 4.8:1

Location of data generally, 3.8

Μ

MAPI e-mail systems, 5.6

Market reports, hearsay exception, 18.3:4

Masters in chancery. See Special masters

Mediation of disputes

generally, 17.3 approach, 17.4:3 benefits, 17.4 compatibility, 17.4:9 costs, 17.4:6, 17.6 data mapping, 17.4:4 deposition transcripts, use, 17.4:1 inaccessbility, 17.4:10 issues, 17.3, 17.4 materials needed, 17.4:2 participants, 17.4:1 position statement, 17.4, 17.4:2 preparation, 17.3 privilege, 17.4:8 procedure generally, 17.4 searches, 17.4:11 selection of mediator, 17.2, 17.5 spoliation, 17.4:5 timing, 17.4:7

Medial information and privacy issues, 24.6:1

Meet and confer

generally, 6.6 admissibility issues, 6.6:1 agenda, 6.7 attendees, 6.2:2 benefits, 6.9 checklists, 5.8, 6.2:3 cooperation, 5.8, 6.8 criminal cases, ESI protocol, 25.3 data sampling, 6.6:3 expert discovery, 6.6:5 federal rule, 5.8, 6.2 form of production, 6.3 keyword searching, 6.6:2 phased discovery, 6.6:4 predictive coding, 6.6:2 preparation, 6.7 preservation agreements, 6.4 privilege issues, 6.5 proposed discovery plan, 6.2:4 purpose, 5.8, 6.2, 6.7 Texas law, 6.1 third party involvement, 6.7 timing, 6.2:1 tone, 6.7 work product issues, 6.5

Mental examinations, 21.7, 21.12

Metadata capturing, 5.10 criminal cases, 25.7:4 defined, 5.5, 25.7:4 duty to preserve, 1.9 e-mail, 5.5, 5.10 ethical issues, 18.3:5, 19.3:4 filtering uses, 8.6:4 production, 9.2:6

Microsoft Exchange, 5.6

Mobile devices characteristics, 26.2:5 definition, 26.2:1, 26.2:2, 26.2:3 discovery requests, 26.2:8 environment, 26.2:6 litigation, 26.2:7 technology, 26.2:4

Motor vehicle ownership records, 24.6:6

Multipurpose Internet Mail Extensions (MIME), 11.6

Native format

Essentials of E-Discovery

N

Native format, 6.3, 9.1, 9.3:4, 9.4:1, 9.4:3, 9.5, 25.8:6

Network adapter, 4.7

Network connections, 7.3:3

N-Gram, 11.16:7

Nonhearsay

admissions by party-opponent, 18.3:5 computer-generated writings, 18.3:5 emoji/emoticon, 18.3:6 metadata, 18.3:5 nonstatements, 18.3:5

Nonparty discovery

authentication, 21.2:4 costs, 21.3, 21.9:4 depositions, 21.2:3, 21.5, 21.10 entry on property, 21.7, 21.11 federal, 21.8 mental examinations, 21.6, 21.12 methods generally, 21.2 notice, 21.4, 21.5, 21.10:2 physical examinations, 21.12 presuit, 21.5 production of electronically stored information in federal court, 21.9:3, 21.9:4 subpoena, 21.2, 21.9 Texas, 21.2

Normalization, 11.11

0

Objections

depositions, 16.4:4 undue burden or cost, 13.2:1

Occupational Safety and Health Act, records retention requirements, 1.3

Octet Streams, 11.6:2

Optical character recognition (OCR), 11.16:8

P

Parent-child relationship, 11.9

Parsing, 11.13

Peer-to-peer networks, 4.8:1

Personal jurisdiction cases, 20.5, 23.2:1

Personal technology devices litigation hold, applicability, 3.2, 3.2:6, 3.2:10 precautions, 3.2 smart phones, 4.7 terminated employees, 3.2:11 white-listing, 3.2:12

Personnel records, 24.7

Phased discovery, 6.6:4

Photographs, authentication, 18.2:21

Physical examinations, 21.12

Physician-patient privilege, 24.6:1, 24.7

Policies for record retention. See Document retention policies (DRPs)

POP3 e-mail systems, 5.6, 7.2:5

Portable document format (PDF), 6.3, 9.2:2

Possession, 26.1:10

Precision, 8.2:1, 8.5:1

Predictive coding generally, 10.1 accuracy, measuring, 10.14 algorithms, 10.1 attorney review, 10.3 benefits, 10.5 choice of parties, 10.15:1 control set, 10.8

Production of electronically stored information

Subject Index

cooperation needed, 8.9:2, 10.13 confidence levels, 10.14 courts' support, 10.15 culling, 10.7 defined, 10.1 disclosure of seed set, 10.13 process generally, 10.11 production of documents, 10.12 quality control, 10.9 seed set, 10.6, 10.13 specialist needed, 10.2 suitability, 10.4 training the computer, 10.8 transparency required, 10.15 vendors, 10.2

Present sense impression, 18.3:3

Preservation agreements, 6.4

Preservation of electronically stored information. See Duty to preserve Privacy issues bank account information, 22.6, 24.3:1, 24.6:6

cell phone records, 24.6:6 computer usage policies, 3.2 confidentiality agreements, 19.2:3, 24.7 constitutional protection (Texas), 24.1 data, 26.1:11 federal laws affecting, 24.5 federal rule generally, 24.2 filings under seal, 24.2:3 financial information, 24.6:3 forensic examinations, 22.6 hard drives, 24.6:5 insurance policyholder information, 24.6:6 international data protection, 24.8 medical information, 24.6:1 motor vehicle ownership records, 24.6:6 personnel records, 24.6:6 protective orders, 24.7 redaction of information, 24.2, 24.3, 24.7 securities purchases, 24.6:6 social media, 24.6:6 stockholder status, 24.6:6 tax returns, 24.6:3

Texas rule generally, 24.3 Privilege generally, 6.5 defined, 12.1 depositions, 16.4:3 eliminating privileged material, 8.2:3, 8.9:2 inadvertent disclosure of privileged material (see Inadvertent disclosure) international issues, 23.5:2 mediation, 17.4:8 physician-patient, 24.6:1, 24.7 waiver (see Waiver of privilege by inadvertent disclosure) Production of electronically stored information. See also Relevant information, identifying ambiguous, 13.2:2 burden, 13.2:2 criminal cases, ESI Protocol, 25.1:3, 25.3 deficient production, Texas state courts. 13.3 existing information requirement, Texas state courts, 13.3:1 failure to produce, 13.2:1 federal rule, 9.3, 13.2 format (see Form of production) inadequate production, Texas state courts, 13.3 inspection, 9.3:1 metadata, 9.2:6 nonparties, 13.2:4 objection, 13.2:2 omissions, 13.3 organization, 9.2:5, 9.3:2 procedure, 9.2:1 processing, 11.17 requirements, 13.2:2, 13.3:2 responses to request, options, 9.2:3, 13.2:2, 13.3:2 scope of discovery, 13.2:1 Texas rule, 13.3 undue burden or cost (see Undue burden or cost) vague, 13.2:2

waiver of objection, 13.2:2

Protective orders

Essentials of E-Discovery

Protective orders

criminal law, 25.9 depositions, 16.3:2 international issues, 23.4:2, 24.8 privacy protection, 24.2:2, 24.7 Texas rule, 24.3:2

Public Information Act, 24.6:2

R

RAID arrays, 4.3:7

Random access memory (RAM), 4.7

Reasonable precision, 8.2:1

Reasonable recall, 8.2:1

Recall, 8.2:1, 8.5:1

Recollection recorded, 18.3:4

Recommendations for electronically stored information (ESI) discovery protection in federal criminal cases. See ESI protocol, criminal cases

Recursion, 11.8

Redaction of information, 24.2:2, 24.2:3, 24.3:1, 24.7

Relevance, defined, 1.5, 1.6, 3.4

Relevant information, identifying

generally, 7.1 backup practices, 7.3:5 custodian interviews, generally, 7.2, 7.3 data map, 7.2:4, 17.4:4 data storage, 7.3:5 document retention policy, 1.4 file servers, 7.2:4 format of data, 7.3:4 former employees, 3.2:11, 7.2:3 instant messages, 7.2:7 IT interviews, generally, 7.2:1 locations, list, 7.2:7 network connections, 7.3:3 social networks, 7.2:7 software used, 7.3:2 technology systems, 7.2:5 voicemails, 7.2:7 workstations, individual, 7.3:1

Remote wiping, 26.1:12

Request for production generally, 9.2:2 inspection, 9.3:1 procedure, 9.2:1 specificity required, 9.2:2, 9.3, 13.2, 13.3, 21.4 Texas rule, 9.2, 13.3

Response to request for electronically stored information. See Production of electronically stored information

Retention of records

federal statutes, 1.3 policies (*see* Document retention policies (DRPs)) policies, 1.4 Texas statutes, 1.3

Reviewing electronically stored information generally, 8.1, 8.11 defined, 8.11:1 e-mails, 5.10 ethical issues, 19.3:2 feedback opportunities, 8.11:6 guidance materials, 8.11:3 hands-on, 8.6:1 linear, 8.6:1 location, 8.11:4 logistics, 8.11:4 manual, 8.6:1 on-site vs. off-site, 8.11:4 outsourcing, 19.3:2 priorities, setting, 8.11:2 process generally, 8.11:2 progress reports, 8.11:6 project management, 8.11:3 protocols, 8.11:3 purpose, 8.11:1

quality control, 8.11:7 reference materials, 8.11:4 scope, 8.11:2 strategy, 8.11:3 status reports, 8.11:6 team, 8.11:3, 8.11:4 technologies, selecting, 8.11:3 timelines, 8.11:3 training, 8.11:4 vendors, 8.11:3

Routine destruction of data. See Document retention policies (DRPs)

Rule 26(f) conference. See Meet and confer

S

Sanctions

generally, 1.1 appellate review, 15.2 cost shifting, 14.2:6 denial, 15.3:11 deposition offenses, 16.1, 16.3, 16.4, 16.5 dismissal of suit, 15.3:9 ethics, 19.2 jury instruction, adverse, 15.3:11 limited award, 15.3:11 negligence, 15.2:9 prejudiced requests, 15.3:8 preservation of data, 1.9, 2.2, 3.1 purpose, 15.1 Texas state court, 15.3:11

Scope of discovery, 8.9, 13.2

Search term calibration, 8.9:2

Searching electronically stored information benefits, 8,7

Boolean searches, 8.6:5 calibration, 8.9:2 case law, 8.9:2 clustering, 8.8:1 complex search, 8.6:5

concept searching, 8.8:2 cooperation needed, 8.9:2 data filtering, 8.6:4 deduplication, 8.6:3 defined, 8.1 false negative, 8.5:3 false positive, 8.5:2 Freedom of Information Act requests, 8.9:2 generally, 8.1 hit report, 8.5:2 keyword, 6.6:2, 8.6:5 limitations, 8.7 metadata, 8.6:4 precision, 8.5:1 predictive coding (see Predictive coding) privileged material, eliminating, 8.10:1 process, 8.1 proportionality, 8.2:2, 8.9:3 recall, 8.5:1 regulatory guidelines, 8.9:1 sampling, 8.5:6 scope of search allowed, 8.1 similarity grouping, 8.8:1 simple search, 8.5:6 statutory guidelines, 8.9:1 stemming, 8.6:5 system file filtering, 8.6:2 technology-assisted review, 8.5:5 visual mapping, 8.8:3 wildcard search, 8.6:5 work product protection of search terms, 8.10:2

Securities purchases, 24.6:6

Self-authentication, 18.2

Servers generally, 4.8 applications, 4.8:3 cloud, 4.8:1 data maps, 7.2:4, 17.4:4 defined, 4.8 e-mail, 5.6 file, 7.2:4 forensic examination, 22.16 inventory, 4.10

Servers

Servers

local, 4.8:1 network shares, 4.9 peer-to-peer, 4.8:1 virtual, 4.8:2

Shingle generation, 11.16:7

Simple container, 11.8:4

Simple document, 11.8:1

Simple keyword search, 8.6:5

Smart phone data, 24.6:6

Snap-back provisions, 10.12, 12.2

Sneak peek agreements, 12.7

Social media and networking sites

admissibility, 20.2 attorneys' use generally, 20.1, 20.4, 20.10 authentication, 18.2:12, 18.2:13 criminal law, 20.10 deletion of postings, 20.5 discovery generally, 20.2 employment law, 20.1 ethics issues, 19.4, 20.8 evidence, use as, 20.7 hearsay issues, 18.3:3, 18.3:5, 20.10 judges' use, 20.8 jurors' use, 20.9 jury selection, 20.9 lawyers' use generally, 20.1, 20.10 personal jurisdiction issues, 20.6 preservation, 20.4, 20.5 prevalance, 20.1 privacy issues generally, 24.6:4 providers, subpoenas for data, 20.3 site policies, 20.3 Stored Communications Act, 20.3

Software, 7.3:2

Solid-state drives, 4.3:6

Sound card, 4.7

Special masters, 17.7

Essentials of E-Discovery

Spoliation of evidence

bad faith, 3.5 burden of proof, 15.2:6 cumulative evidence, 15.3:11 defined, 3.5 good faith, effect, 3.5 intentional, 15.2:7, 15.3:5 litigation hold, 2.2 negligent vs. willful, 15.2:7, 15.3:6 prejudice, resulting, 15.3:8 procedure, Texas state court, 15.3 reckless, 15.3:7 sanctions (*see* Sanctions) Texas federal court, 15.2 Texas state court, 15.3

Stemming keyword search, 8.6:5

Stockholder status, 24.6:6

Storage media flash drives, 4.3:6 generally, 4.3:6 hard drives, 4.3:6 RAID arrays, 4.3:7 solid-state drives, 4.3:6

Stored Communications Act, 20.3

Stored data, authentication, 18.2:5

Structured document, 11.8:2

Subpoenas federal rule, 21.9 nonparties generally, 21.2:1, 21.2:2 social media providers, 20.2, 20.3, 24.6:4

Т

Tagged image file format (TIFF), 6.3, 9.4:2, 9.6, 11.15

Tax returns and privacy issues, 24.6:3

Terminology. See Computer terminology; Definitions

Texas health privacy law, 26.1:11

Workstations

Texas Public Information Act, 24.6:1, 24.6:2

Text messages authentication, 18.2:9 privacy concerns, 20.3

Text structures, 11.6:2

Third-party-held documents, 1.12

Tokenization, 11.13

U

Undue burden or cost generally, 13.2:1, 14.1 burden of proof, 13.2, 14.2, 21.9:2, 23.2:2, 24.6:3 cost-benefit analysis, 14.2:2, 21.9:4 factors, 14.2:2 federal rule, 13.2:4, 14.2 good cause, effect, 13.2 grounds, 14.2:2 market knowledge required, 14.2:2 objection, specificity required, 13.2:2, 14.2 options for addressing, 13.2 proportionality rule, 14.2:2 sampling as a solution, 13.2 vendor quotes as evidence, 14.2:3, 19.2:5

Unfair prejudice, 18.4

USB drives, 4.3:6

V

Videos, authentication, 18.2:17, 18.2:21

Virtual private networks, 3.2:13 Virtual servers, 4.8:2 Virus scanning, 11.16:9 Visual mapping, 8.8:3 Voicemails, 6.4, 18.2:22, 18.2:23

W

Waiver of privilege by inadvertent disclosure generally, 12.1 failure to promptly rectify error, 12.4:3 federal rule generally, 12.6, 12.7 protective orders, 12.7 Texas rule, 12.2

Web site postings, authentication, 18.2:10

White-listing, 3.2:12

Wildcard keyword search, 8.6:5

Work product protection generally, 6.5, 8.10:2 defined, 8.10:2 depositions, 16.4 international issues, 23.5:2 litigation hold memorandum, 2.5 search terms, 8.10:2 waiver (*see* Waiver of privilege by inadvertent disclosure)

Workstations, 7.3:1



How to Download This Book

To install this book's digital download-

- 1. go to https://manage.texasbarpractice.com;
- 2. if prompted to log in, do so; and
- 3. in the "Downloadables" column, click the download button for this book's title.

For details, see the section below titled "Downloading and Installing."

DIGITAL DOWNLOAD DOCUMENTATION

Essentials of E-Discovery, Second Edition Digital Download 2021

The complimentary downloadable version of *Essentials of E-Discovery*, second edition, contains the entire text of the printed book. If you have questions or problems with this product not covered in the documentation available via the URLs below, please contact Texas Bar Books at 800-204-2222, ext. 1499 for technical support or ext. 1411 for orders and accounts, or at **books@texasbar.com**.

Additional and Entity Licenses

The current owner of this book may purchase additional and entity licenses for the digital download. Each additional license is for one additional lawyer and that lawyer's support team only. Additional and entity licenses are subject to the terms of the original license concerning permitted users of the printed book and digital download. Please visit **www.texasbarpractice.com/knowledgebase/article/how-to-get-access-for-other**-lawyers for details.

Usage Tips and Other Information

For information on digital download licensing, installation, and usage, visit the Texas Bar Practice Knowledge Base at www.texasbarpractice.com/knowledgebase.

Downloading and Installing

Use of the digital download is subject to the terms of the license and limited warranty included in this documentation and on the digital download web pages. By accessing the digital download, you waive all refund privileges for this publication.

How to Download This Book

To install this book's complete digital download, follow the instructions below.*

1. Go to https://manage.texasbarpractice.com:

If the site prompts you to log you in, do so using the email address associated with this purchase.

Signin × +		×
← → C △ ▲ https://manage.texasbarpractice.com		\$ 1
	Exast Base Bign in with your email and password Email mane@host.com Password Password Forgot your password?	

Once logged in, you should see the user icon in the upper right-hand corner of the page.



2. Go to your account:



3. Select the library of the individual cr organization associated with this download, and click the download button rext to the book's title.

Home Page - TexasBarAssociatio X +					- 0
* TEXAS BAR	PRACTICE TEXAS BAR B	IOOKS LAW PRAC	TICE MANAGEMENT		
TEXAS BAR PRACTICE Blog A	bout Us Bookshop				۲
My Library My Profile Subscriptions / Auto-R	enewals Order History	Organizations	Payment Methods Pay	My Bill	
My Library			My Library		-
SUBSCRIPTIONS		DOWNL	OADABLES		
				-	
Texas Business Organizations Manual Online	Go to Product			. 0	ownload
Texas Business Organizations Manual Online Texas Collections Manual Online	Go to Product Go to Product	Texas Business C	rganizations Manual, 2020	ed. D	ownload &
Texas Business Organizations Manual Online Texas Collections Manual Online Texas Family Law Practice Manual Online	Go to Product Go to Product Go to Product	Texas Business C	rganizations Manual, 2020	ed. D	ownload

*Notes:

- If you have never logged in to our site, the purchaser of this book should follow the instructions at www.texasbarpractice.com/knowledgebase/article/ already-a-customer.
- If you purchased the book as an organization, see www.texasbarpractice.com/ knowledgebase/texas-bar-practice-accounts.

If you need any assistance, you may chat with us online or email us at **books@texasbar.com**.

USE OF THE MATERIAL IN THE DIGITAL DOWNLOAD IS SUBJECT TO THE FOLLOWING LICENSE AGREEMENT.

License and Limited Warranty

Grant of license: The material in the digital product and in the documentation is copyrighted by the State Bar of Texas ("State Bar"). The State Bar grants you a nonexclusive license to use this material as long as you abide by the terms of this agreement.

Ownership: The State Bar retains title and ownership of the material in the files and in the documentation and all subsequent copies of the material regardless of the form or media in which or on which the original and other copies may exist. This license is not a sale of the material or any copy. The terms of this agreement apply to derivative works.

Permitted users: The material in these files is licensed to you for use by one lawyer and that lawyer's support team only. At any given time, the material in these files may be installed only on the computers used by that lawyer and that lawyer's support team. That lawyer may be the individual purchaser or the lawyer designated by the firm that purchased this product. You may not permit other lawyers to use this material unless you purchase additional licenses. **Lawyers, law firms, and law firm librarians are specifically prohibited from distributing these materials to more than one lawyer.** A separate license must be purchased for each lawyer who uses these materials. For information about special bulk discount pricing for law firms, please call 1-800-204-2222, ext. 1402, or 512-427-1402. Libraries not affiliated with firms may permit reading of this material by patrons of the library through installation on one or more computers owned by the library and on the library's network but may not lend or sell the files themselves. The library may not allow patrons to print or copy any of this material in such a way as would infringe the State Bar's copyright.

Copies: You may make a copy of the files for backup purposes. Otherwise, you may copy the material in the files only as necessary to allow use by the users permitted under the license you purchased. Copyright notices should be included on copies. You may copy the documentation, including any copyright notices, as needed for reference by authorized users, but not otherwise.

Transfer: You may not transfer any copy of the material in the files or in the documentation to any other person or entity unless the transferee first accepts this agreement in writing and you transfer all copies, wherever located or installed, of the material and documentation, including the original provided with this agreement. You may not rent, loan, lease, sublicense, or otherwise make the material available for use by any person other than the permitted users except as provided in this paragraph.

Limited warranty and limited liability: THE STATE BAR MAKES NO WARRANTIES, EXPRESS OR IMPLIED, CONCERNING THE MATERIAL IN THESE FILES, THE DOCU-MENTATION, OR THIS AGREEMENT. THE STATE BAR EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABIL-ITY AND OF FITNESS FOR A PARTICULAR PURPOSE. THE MATERIAL IN THE FILES AND IN THE DOCUMENTATION IS PROVIDED "AS IS."

THE STATE BAR SHALL NOT BE LIABLE FOR THE LEGAL SUFFICIENCY OR LEGAL ACCURACY OF ANY OF THE MATERIAL CONTAINED IN THESE FILES. NEITHER THE STATE BAR NOR ANY OF THE CONTRIBUTORS TO THE MATERIAL MAKES EITHER EXPRESS OR IMPLIED WARRANTIES WITH REGARD TO THE USE OR FREEDOM FROM ERROR OF THE MATERIAL. EACH USER IS SOLELY RESPONSIBLE FOR THE LEGAL EFFECT OF ANY USE OR MODIFICATION OF THE MATERIAL.

IN NO EVENT SHALL THE STATE BAR BE LIABLE FOR LOSS OF PROFITS OR FOR INDIRECT, SPECIAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, EVEN IF THE STATE BAR HAS BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES. THE STATE BAR'S AGGREGATE LIABILITY ARISING FROM OR RELATING TO THIS AGREEMENT OR THE MATERIAL IN THE FILES OR IN THE DOCUMENTATION IS LIMITED TO THE PURCHASE PRICE YOU PAID FOR THE LICENSED COPYRIGHTED PRODUCT. THIS AGREEMENT DEFINES YOUR SOLE REMEDY.

General provisions: This agreement contains the entire agreement between you and the State Bar concerning the license to use the material in the files. The waiver of any breach of any provision of this agreement does not waive any other breach of that or any other provision. If any provision is for any reason found to be unenforceable, all other provisions nonetheless remain enforceable.





ESSENTIALS OF E-DISCOVERY

magine how our lives have changed in just one generation. Few students graduating from law school now have any memory of life before personal computers, smart phones, e-mail, text messaging, or online legal research. Few lawyers who graduated from law school before 1984 had to deal with information technology more sophisticated than an electric typewriter before they were called to the bar. While we have come to expect that all large enterprises rely on computer systems and the data those systems generate and store, it has only been in the past few years that we have come to realize that digital information technology touches every aspect of our lives. From the corporate merger to the common divorce, from the complex securities fraud action to the speeding ticket, nearly every case brought to today's law office will involve some electronically stored information. I commend the Honorable Xavier Rodriguez for undertaking to assemble, in one volume, these *Essentials of E-Discovery*.

Ken Withers Deputy Executive Director The Sedona Conference

ABOUT THE EDITOR

udge Xavier Rodriguez is a former Texas Supreme Court Justice and currently sits on the bench as a United States District Judge for the Western District of Texas. Born in San Antonio, he received his bachelor's degree from Harvard University, a master's degree from the University of Texas LBJ School of Public Affairs, and a J.D. from the University of Texas School of Law. Judge Rodriguez is a frequent speaker on continuing legal education seminars and has authored numerous articles regarding employment law, discovery, and arbitration issues, and was the editor of the 2014 edition of Essentials of E-Discovery. He is a member of The Sedona Conference Judicial advisory board and the Georgetown Advanced E-Discovery Institute advisory board, and serves as the Distinguished Visiting Jurist-in-Residence and adjunct professor of law at St. Mary's University School of Law. He was elected to membership in the American Law Institute and is a fellow of the American Bar Foundation and the Texas Bar Foundation. In 2011, he was awarded the Rosewood Gavel Award for outstanding judicial service from St. Mary's University School of Law. In 2017, he received the State Bar of Texas Gene Cavin Award for Excellence in CLE, recognizing his long-term contributions to continuing legal education. He is a past chair of the State Bar of Texas Continuing Legal Education Committee and of the State Bar of Texas Litigation Section. He is currently enrolled in the Duke University Bolch Judicial Institute's LLM Program in Judicial Studies. ISBN 978-1-938873-83-6





6555