

Texas Law Review

SYMPOSIUM:

LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY

Matthew A. Anzaldi & Jonathan W. Gannon

William C. Banks

Lisa Graves

Eric Talbot Jensen

Alexander W. Joel

Sean Kanuck

Orin S. Kerr

Heidi Kitrosser

Jon D. Michaels

Paul Ohm

Nicholas J. Patterson

Afsheen John Radsan

Samuel J. Rascoff

Nathan Alexander Sales

Stephen I. Vladeck

Texas Law Review

A national journal published seven times a year

Recent and Forthcoming Articles of Interest

THE INCENTIVES MATRIX:
THE COMPARATIVE EFFECTIVENESS OF REWARDS, LIABILITIES,
DUTIES, AND PROTECTIONS FOR REPORTING ILLEGALITY

Yuval Feldman & Orly Lobel

May 2010

KEEP CHARITY CHARITABLE

Brian Galle

May 2010

THE TAKING/TAXING TOXONOMY

Amnon Lehavi

May 2010

NO MORE TINKERING:
THE ALI AND THE DEATH PENALTY
PROVISIONS OF THE MODEL PENAL CODE

Carol S. Steiker & Jordan M. Steiker

November 2010

REGULATORY ARBITRAGE

Victor Fleischer

December 2010

Individual issue rate: \$15.00 per copy

Subscriptions: \$47.00 (seven issues)

Order from:

**School of Law Publications
University of Texas at Austin
727 East Dean Keeton Street
Austin, Texas USA 78705**

(512) 232-1149

<http://www.texaslawpublications.com>

TEXAS LAW REVIEW ASSOCIATION

OFFICERS

GREGORY S. COLEMAN
President-Elect

CARRIN F. PATMAN
President

NICK S. DHESI
Executive Director

JAMES A. HEMPHILL
Treasurer

BRANDON C. JANES
Immediate Past President

BOARD OF DIRECTORS

NINA CORTELL
KARL G. DIAL
GARY L. EWELL
R. JAMES GEORGE, JR.
DIANA M. HUDSON

JEFFREY C. KUBIN
D. MCNEEL LANE
LEWIS T. LECLAIR
JOHN B. MCKNIGHT
MICHAEL H. NEWMAN
ERIC J.R. NICHOLS

DAVID M. RODI
REAGAN W. SIMPSON
MOLLY STEELE
MARK L.D. WAWRO
HON. DIANE P. WOOD

SCOTT J. ATLAS, *ex officio Director*
BRICE A. WILKINSON, *ex officio Director*

Texas Law Review (ISSN 0040-4411) is published seven times a year—November, December, February, March, April, May, and June. The annual subscription price is \$47.00 except as follows: Texas residents pay \$50.88 and foreign subscribers pay \$55.00. All publication rights are owned by the Texas Law Review Association. *Texas Law Review* is published under license by The University of Texas at Austin School of Law, P.O. Box 8670, Austin, Texas 78713. Periodicals Postage Paid at Austin, Texas, and at additional mailing offices.

POSTMASTER: Send address changes to The University of Texas at Austin School of Law, P.O. Box 8670, Austin, Texas 78713.

Complete sets and single issues are available from WILLIAM S. HEIN & Co., INC., 1285 Main St., Buffalo, NY 14209-1987. Phone: 1-800-828-7571.

Single issues in the current volume may be purchased from the *Texas Law Review* Publications Office for \$15.00 per copy plus shipping. Texas residents, please add applicable sales tax.

The *Texas Law Review* is pleased to consider unsolicited manuscripts for publication but regrets that it cannot return them. Please submit a single-spaced manuscript, printed on one side only, with footnotes rather than endnotes. Citations should conform with the *Texas Rules of Form* (11th ed. 2006) and *The Bluebook: A Uniform System of Citation* (18th ed. 2005). Except when content suggests otherwise, the *Texas Law Review* follows the guidelines set forth in the *Texas Law Review Manual on Usage & Style* (11th ed. 2008), *The Chicago Manual of Style* (15th ed. 2003), and Bryan A. Garner, *A Dictionary of Modern Legal Usage* (2d ed. 1995).

Except as otherwise noted, the *Texas Law Review* is pleased to grant permission for copies of articles, notes, and book reviews to be made for classroom use, provided that (1) a proper notice of copyright is affixed to each copy, (2) the author and source are identified, (3) copies are distributed at or below cost, and (4) the Texas Law Review Association is notified of the use.

© Copyright 2010, Texas Law Review Association

Editorial Offices: *Texas Law Review*
727 East Dean Keeton Street, Austin, Texas 78705
(512) 232-1280 Fax (512) 471-3282
tr@law.utexas.edu
<http://www.texaslrev.com>

THE UNIVERSITY OF TEXAS SCHOOL OF LAW

ADMINISTRATIVE OFFICERS

LAWRENCE G. SAGER, B.A., LL.B.; *Dean, John Jeffers Research Chair in Law, Alice Jane Drysdale Sheffield Regents Chair.*
MECHELE DICKERSON, B.A., J.D.; *Associate Dean for Academic Affairs, Arthur L. Moller Chair in Bankruptcy Law and Practice.*
ALEXANDRA W. ALBRIGHT, B.A., J.D.; *Associate Dean for Administrative Services, Senior Lecturer.*
EDEN E. HARRINGTON, B.A., J.D.; *Assistant Dean for Clinical Education, Director of William Wayne Justice Center for Public Interest Law.*
KIMBERLY L. BIAR, B.B.A.; *Assistant Dean for Financial Affairs, Certified Public Accountant.*
CARLA COOPER, B.A., M.A., Ph.D.; *Assistant Dean for Alumni Relations and Development.*
MICHAEL J. ESPOSITO, B.A., J.D., M.B.A.; *Assistant Dean for Continuing Legal Education.*
KIRSTON FORTUNE, B.F.A.; *Assistant Dean for Communications.*
MONICA K. INGRAM, B.A., J.D.; *Assistant Dean for Admissions and Financial Aid.*
DAVID A. MONTOTO, B.A., J.D.; *Assistant Dean for Career Services.*
LESLIE OSTER, B.A., J.D.; *Assistant Dean for Strategic Planning.*
REYMUNDO RAMOS, B.A.; *Assistant Dean for Student Affairs.*

FACULTY EMERITI

HANS W. BAADE, A.B., J.D., LL.B., LL.M.; *Hugh Lamar Stone Chair Emeritus in Civil Law.*
RICHARD V. BARNDT, B.S.L., LL.B.; *Professor Emeritus.*
WILLIAM W. GIBSON, JR., B.A., LL.B.; *Sylvan Lang Professor Emeritus in Law of Trusts.*
ROBERT W. HAMILTON, A.B., J.D.; *Minerva House Drysdale Regents Chair Emeritus.*
DOUGLAS LAYCOCK, B.A., J.D.; *Alice McKean Young Regents Chair Emeritus.*
J. L. LEBOWITZ, A.B., J.D., LL.M.; *Joseph C. Hutcheson Professor Emeritus.*
JOHN T. RATLIFF, JR., B.A., LL.B.; *Ben Gardner Sewell Professor Emeritus in Civil Trial Advocacy.*
JOHN F. SUTTON, JR., J.D.; *A.W. Walker Centennial Chair Emeritus.*
JAMES M. TREECE, B.A., J.D., M.A.; *Charles I. Francis Professor Emeritus in Law.*
RUSSELL J. WEINTRAUB, B.A., J.D.; *Ben H. & Kitty King Powell Chair Emeritus in Business and Commercial Law.*

PROFESSORS

JEFFREY B. ABRAMSON, B.A., J.D., Ph.D.; *Professor of Law and Government.*
DAVID E. ADELMAN, B.A., Ph.D., J.D.; *Harry Reasoner Regents Chair in Law.*
DAVID A. ANDERSON, A.B., J.D.; *Fred and Emily Marshall Wulff Centennial Chair in Law.*
MARK L. ASCHER, B.A., M.A., J.D., LL.M.; *Joseph D. Jamail Centennial Chair in Law.*
RONEN AVRAHAM, M.A., LL.M., J.S.D.; *Thomas Shelton Maxey Professor in Law.*
LYNN A. BAKER, B.A., Honours B.A., J.D.; *Frederick M. Baron Chair in Law, Co-Director of Center on Lawyers, Civil Justice, and the Media.*
MITCHELL N. BERMAN, A.B., M.A., J.D.; *Richard Dale Endowed Chair in Law.*
BERNARD S. BLACK, A.B., M.A., J.D.; *Hayden W. Head Regents Chair for Faculty Excellence, Director of Center for Law, Business, and Economics.*
LYNN E. BLAIS, A.B., J.D.; *Leroy G. Denman, Jr. Regents Professor in Real Property Law.*
ROBERT G. BONE, B.A., J.D.; *Professor.*
NORMA V. CANTU, B.A., J.D.; *Professor of Law and Education.*
LOFTUS C. CARSON, II, B.S., M. Pub. Aff., M.B.A., J.D.; *Ronald D. Krist Professor.*
ROBERT M. CHESNEY, B.S., J.D.; *Charles I. Francis Professor in Law.*
MICHAEL J. CHURGIN, A.B., J.D.; *Raybourne Thompson Centennial Professor.*
JANE M. COHEN, B.A., J.D.; *Edward Clark Centennial Professor.*
FRANK B. CROSS, B.A., J.D.; *Herbert D. Kelleher Centennial Professor of Business Law.*
JOHN DEIGH, B.A., M.A., Ph.D.; *Professor of Law and Philosophy.*
GEORGE E. DIX, B.A., J.D.; *George R. Killam, Jr. Chair of Criminal Law.*
JOHN S. DZIENKOWSKI, B.B.A., J.D.; *Dean John F. Sutton, Jr. Chair in Lawyering and the Legal Process.*
KAREN L. ENGLE, B.A., J.D.; *Cecil D. Redford Professor in Law, Director of Bernard and Audre Rapoport Center for Human Rights and Justice.*
WILLIAM E. FORBATH, A.B., B.A., Ph.D., J.D.; *Lloyd M. Bentsen Chair in Law.*
JULIUS G. GETMAN, B.A., LL.B., LL.M.; *Earl E. Sheffield Regents Chair.*
STEVEN GOODE, B.A., J.D.; *W. James Kronzer Chair in Trial and Appellate Advocacy, University Distinguished Teaching Professor.*
LINO A. GRAGLIA, B.A., LL.B.; *A. Dalton Cross Professor.*
PATRICIA I. HANSEN, A.B., M.P.A., J.D.; *J. Waddy Bullion Professor.*
HENRY T. HU, B.S., M.A., J.D.; *Allan Shivers Chair in the Law of Banking and Finance.*
DEREK P. JINKS, B.A., M.A., J.D.; *The Marrs McLean Professor in Law.*
STANLEY M. JOHANSON, B.S., LL.B., LL.M.; *Fannie Coplin Regents Chair, University Distinguished Teaching Professor.*
CALVIN H. JOHNSON, B.A., J.D.; *Andrews & Kurth Centennial Professor.*
SUSAN R. KLEIN, B.A., J.D.; *Alice McKean Young Regents Chair in Law.*
SANFORD V. LEVINSON, A.B., Ph.D., J.D.; *W. St. John Garwood and W. St. John Garwood, Jr. Centennial Chair in Law, Professor of Government.*
STEFANIE A. LINDQUIST, B.A., J.D., Ph.D.; *The Thomas W. Gregory Professorship in Law.*
BASIL S. MARKESINIS, LL.B., LL.D., DCL, Ph.D.; *Jamail Regents Chair.*
INGA MARKOVITS, LL.M.; *"The Friends of Joe Jamail" Regents Chair.*
RICHARD S. MARKOVITS, B.A., LL.B., Ph.D.; *John B. Connally Chair.*
THOMAS O. MCGARITY, B.A., J.D.; *Joe R. and Teresa Lozano Long Endowed Chair in Administrative Law.*
LINDA S. MULLENIX, B.A., M. Phil., J.D., Ph.D.; *Morris & Rita Atlas Chair in Advocacy.*

ROBERT J. PERONI, B.S.C., J.D., LL.M.; *James A. Elkins Centennial Chair in Law*.
H. W. PERRY, JR., B.A., M.A., Ph.D.; *Associate Professor of Law and Government*.
LUCAS A. POWE, JR., B.A., J.D.; *Anne Green Regents Chair in Law, Professor of Government*.
WILLIAM C. POWERS, JR., B.A., J.D.; *President, The University of Texas at Austin, Hines H. Baker and Thelma Kelley Baker Chair, University Distinguished Teaching Professor*.
DAVID M. RABBAN, B.A., J.D.; *Dahr Jamail, Randall Hage Jamail, and Robert Lee Jamail Regents Chair, University Distinguished Teaching Professor*.
ALAN S. RAU, B.A., LL.B.; *Burg Family Professorship*.
R. A. REESE, B.A., J.D.; *Arnold, White & Durkee Centennial Professor*.
DAVID W. ROBERTSON, B.A., LL.B., LL.M., J.S.D.; *W. Page Keeton Chair in Tort Law, University Distinguished Teaching Professor*.
JOHN A. ROBERTSON, A.B., J.D.; *Vinson & Elkins Chair*.
DANIEL B. RODRIGUEZ, B.A., J.D.; *Minerva House Drysdale Regents Chair in Law*.
WILLIAM M. SAGE, A.B., M.D., J.D.; *James R. Dougherty Chair for Faculty Excellence*.
JOHN J. SAMPSON, B.B.A., LL.B.; *William Benjamin Wynne Professor*.
THOMAS K. SEUNG, Ph.D.; *Jesse H. Jones Regents Professor in Liberal Arts*.
MICHAEL M. SHARLOT, B.A., LL.B.; *Wright C. Morrow Professor*.
CHARLES M. SILVER, B.A., M.A., J.D.; *Roy W. and Eugenia C. MacDonald Endowed Chair in Civil Procedure, Co-Director of Center on Lawyers, Civil Justice, and the Media*.
ERNEST E. SMITH, B.A., LL.B.; *Rex G. Baker Centennial Chair in Natural Resources Law*.
JANE STAPLETON, B.S., Ph.D., LL.B., D. Phil.; *Ernest E. Smith Professor*.
JORDAN M. STEIKER, B.A., J.D.; *Judge Robert M. Parker Endowed Chair in Law*.
MICHAEL F. STURLEY, B.A., J.D.; *Stanley D. and Sandra J. Rosenberg Centennial Professor in Property Law*.
SHIRLEY E. THOMPSON, A.B., A.M., Ph.D.; *Professor*.
GERALD TORRES, A.B., J.D., LL.M.; *Bryant Smith Chair in Law*.
GREGORY J. VINCENT, B.A., J.D., Ed.D.; *Professor*.
WENDY E. WAGNER, B.A., M.E.S., J.D.; *Joe A. Worsham Centennial Professor*.
LOUISE WEINBERG, A.B., J.D., LL.M.; *William B. Bates Chair for the Administration of Justice*.
OLIN G. WELLBORN, A.B., J.D.; *William C. Liedtke, Sr. Professor*.
JAY L. WESTBROOK, B.A., J.D.; *Benno C. Schmidt Chair of Business Law*.
ABRAHAM L. WICKELGREEN, A.B., Ph.D., J.D.; *Bernard J. Ward Professor in Law*.
ZIPPORAH B. WISEMAN, B.A., M.A., LL.B.; *Thos. H. Law Centennial Professor in Law*.
PATRICK WOOLLEY, A.B., J.D.; *Beck, Redden & Secrest Professor*.

ASSISTANT PROFESSORS

OREN BRACHA, LL.B., S.J.D.
DANIEL M. BRINKS, A.B., J.D., Ph.D.
JENS C. DAMMANN, J.D., LL.M., Dr. Jur., J.S.D.
JUSTIN DRIVER, B.A., M.A., M.A., J.D.
ZACHARY S. ELKINS, B.A., M.A., Ph.D.
MIRA GANOR, B.A., M.B.A., LL.B., LL.M., J.S.D.
JOHN M. GOLDEN, A.B., J.D., Ph.D.
EMILY E. KADENS, B.A., M.A., Dipl., M.A., Ph.D., J.D.
JENNIFER E. LAURIN, B.A., J.D.
ANGELA K. LITWIN, B.A., J.D.
MARY ROSE, A.B., M.A., Ph.D.
SEAN H. WILLIAMS, B.A., J.D.
HANNAH J. WISEMAN, A.B., J.D.

SENIOR LECTURERS, WRITING LECTURERS, AND CLINICAL PROFESSORS

WILLIAM P. ALLISON, B.A., J.D.; *Clinical Professor, Director of Criminal Defense Clinic*.
MARJORIE I. BACHMAN, B.S., J.D.; *Clinical Instructor*.
PHILIP C. BOBBITT, A.B., J.D., Ph.D.; *Distinguished Senior Lecturer*.
KAMELA S. BRIDGES, B.A., B.J., J.D.; *Lecturer*.
CYNTHIA L. BRYANT, B.A., J.D.; *Clinical Professor, Director of Mediation Clinic*.
SARAH M. BUEL, B.A., J.D.; *Clinical Professor*.
MARY R. CROUTER, A.B., J.D.; *Assistant Director of William Wayne Justice Center for Public Interest Law*.
TIFFANY J. DOWLING, B.A., J.D.; *Clinical Instructor*.
LORI K. DUKE, B.A., J.D.; *Clinical Professor*.
ARIEL E. DULITZKY, J.D., LL.M.; *Clinical Professor*.
DENISE L. GILMAN, B.A., J.D.; *Clinical Professor*.
BARBARA HINES, B.A., J.D.; *Director of Immigration Clinic*.
KRISTINE A. HUSKEY, B.A., J.D.; *Director of National Security & Human Rights Clinic*.
JEANA A. LUNGWITZ, B.A., J.D.; *Clinical Professor, Director of Domestic Violence Clinic*.
ROBIN B. MEYER, B.A., M.A., J.D.; *Lecturer*.
TRACY W. MCCORMACK, B.A., J.D.; *Director of Trial Advocacy Program*.
RANJANA NATARAJAN, B.A., J.D.; *Clinical Professor*.
ROBERT C. OWEN, A.B., M.A., J.D.; *Clinical Professor, Co-Director of Capital Punishment Clinic*.
SEAN J. PETRIE, B.A., J.D.; *Lecturer*.
WAYNE SCHIESS, B.A., J.D.; *Senior Lecturer, Director of Legal Writing*.
PAMELA J. SIGMAN, B.A., J.D.; *Lecturer, Director of Juvenile Justice Clinic*.
LESLIE L. STRAUCH, B.A., J.D.; *Clinical Professor*.
DAVID S. SOKOLOV, B.A., M.A., J.D., M.B.A.; *Distinguished Senior Lecturer, Director of Student Life*.
JAN SUMMER, B.A., M.A., J.D.; *Executive Director of Center for Public Policy Dispute Resolution*.
MELINDA E. TAYLOR, B.A., J.D.; *Senior Lecturer, Executive Director of Center for Global Energy, International Arbitration, and Environmental Law*.
HEATHER K. WAY, B.A., B.J., J.D.; *Lecturer, Director of Community Development Clinic*.
ELIZABETH M. YOUNGDALE, B.A., M.L.I.S., J.D.; *Lecturer*.

ADJUNCT PROFESSORS AND OTHER LECTURERS

WILLIAM R. ALLENSWORTH, B.A., J.D.
 JAMAL K. ALSAFFAR, B.A., J.D.
 MARILYN ARMOUR, B.A., M.S.W., Ph.D.
 WILLIAM G. BARBER, B.S.Ch.E., J.D.
 WILLIAM G. BARBER, III, B.A., LL.M.
 NICOLAS G. BARZOUKAS, B.S., M.B.A., J.D.
 SHARON C. BAXTER, B.S., J.D.
 KATHERINE E. BEAUMONT, B.A., J.D.
 KARA BELEW, B.A., B.B.A., J.D.
 WILLIAM H. BEARDALL, JR., B.A., J.D.
 JERRY A. BELL, B.A., J.D.
 ALLISON H. BENESCH, B.A., M.S.W., J.D.
 CRAIG R. BENNETT, B.S., J.D.
 JAMES B. BENNETT, B.B.A., J.D.
 MELISSA J. BERNSTEIN, B.A., M.L.S., J.D.
 MURFF F. BLEDSOE, B.A., J.D.
 WILLIAM P. BOWERS, B.B.A., J.D., LL.M.
 ANTHONY W. BROWN, B.A., J.D.
 JAMES E. BROWN, LL.B.
 TOMMY L. BROYLES, B.A., J.D.
 PAUL J. BURKA, B.A., LL.B.
 W. A. BURTON, JR., B.A., M.A., LL.B.
 AGNES E. CASAS, B.A., J.D.
 RUBEN V. CASTANEDA, B.A., J.D.
 EDWARD A. CAVAZOS, B.A., J.D.
 CHARLES G. CHILDRESS, B.A., J.D.
 DAN J. CHRISTENSEN, B.B.A., J.D.
 JOSEPH A. CIALONE, II, B.A., J.D.
 JEFF CIVINS, A.B., M.S., J.D.
 JUDGE LEIF M. CLARK, B.A., M.Div., J.D.
 DANA L. COBB, B.A., J.D.
 GARY COBB, B.A., J.D.
 MARK W. COCHRAN, B.J., LL.M., J.D.
 ELIZABETH COHEN, B.A., M.S.W., J.D.
 JAMES W. COLLINS, B.S., J.D.
 TED CRUZ, A.B., J.D.
 PATRICIA J. CUMMINGS, B.A., J.D.
 WILLIAM H. CUNNINGHAM, B.A., M.B.A., Ph.D.
 HECTOR DE LEON, B.S., J.D.
 DICK DEGUERIN, B.A., LL.B.
 MICHELE Y. DEITCH, B.A., M.S., J.D.
 ADAM R. DELL, B.A., J.D.
 CASEY D. DUNCAN, B.A., M.L.I.S., J.D.
 PHILIP DURST, B.A., M.A., J.D., Ph.D.
 ELANA S. EINHORN, B.A., J.D.
 JAY D. ELLWANGER, B.A., J.D.
 LOWELL P. FELDMAN, B.A., J.D.
 KENNETH FLAMM, Ph.D.
 JOHN C. FLEMING, B.A., J.D.
 MARIA FRANKLIN, B.A., M.A., Ph.D.
 DAVID C. FREDERICK, B.A., Ph.D., J.D.
 GREGORY D. FREED, B.A., J.D.
 ELIZABETH FRUMKIN, B.A., M.A., J.D.
 FRED J. FUCHS, B.A., J.D.
 MICHAEL GAGARIN, Ph.D.
 GERALD J. GALOW, B.A., J.D.
 JAMES B. GAMBRELL, B.S.M.E., M.A., LL.B.
 FRANCIS J. GAVIN, B.A., M.S.T., Ph.D.
 CHARLES E. GHOLZ, B.S., Ph.D.
 MICHAEL J. GOLDEN, A.B., J.D.
 JULIE E. GRANTHAM, B.A., J.D.
 SHERRI R. GREENBERG, B.A., M.Sc.
 ROBERT L. GROVE, B.S., J.D.
 DAVID HALPERN, B.A., J.D.
 JETT L. HANNA, B.B.A., J.D.
 KELLY L. HARAGAN, B.A., J.D.
 CLINT A. HARBOUR, B.A., J.D., LL.M.
 AMY J. SCHUMACHER, B.A., J.D.
 AARON R. SCHWARTZ, B.A., LL.B.
 MARCUS F. SCHWARTZ, B.B.A., J.D.
 SUZANNE SCHWARTZ, B.J., J.D.
 ROBERT L. HARGETT, B.B.A., J.D.
 BARBARA J. HARLOW, B.A., M.A., Ph.D.
 JAMES C. HARRINGTON, B.A., M.A., J.D.
 CHRISTOPHER S. HARRISON, Ph.D., J.D.
 AMBER L. HATFIELD, B.S.E.E., J.D.
 JOHN R. HAYS, JR., B.A., J.D.
 PAUL M. HEBERT, A.B., J.D.
 STEVEN L. HIGHLANDER, B.A., Ph.D., J.D.
 SUSAN J. HIGHTOWER, B.A., M.A., J.D.
 WILLIAM M. HINES, III, B.B.A., J.D.
 JAMES C. HO, B.A., J.D.
 KENNETH E. HOUP, JR., J.D.
 RANDY R. HOWRY, B.J., J.D.
 MONTY G. HUMBLE, B.A., J.D.
 BOBBY R. INMAN, B.A.
 PATRICK O. KEEL, B.A., J.D.
 CHARI L. KELLY, B.A., J.D.
 ROBERT N. KEPPLE, B.A., J.D.
 MARK L. KINCAID, B.B.A., J.D.
 KEVIN S. KUDLAC, B.S., J.D.
 KURT H. KUHN, B.A., J.D.
 AMI L. LARSON, B.A., J.D.
 KEVIN R. LASHUS, B.A., J.D.
 JODI R. LAZAR, B.A., J.D.
 MAURIE A. LEVIN, B.A., J.D.
 ANDREW F. MACRAE, B.J., J.D.
 VIJAY MAHAJAN, M.S.Ch.E., Ph.D.
 JIM MARCUS, B.A., J.D.
 PETER D. MARKETOS, B.A., J.D.
 FRANCES L. MARTINEZ, B.A., J.D.
 RAY MARTINEZ, III, B.A., J.D.
 ALOYSIUS P. MARTINICH, B.A., M.A., Ph.D.
 LISA M. MCCLAINE, B.A., J.D., LL.M.
 STEPHANIE G. MCFARLAND, B.A., J.D.
 BARRY F. MCNEIL, B.A., J.D.
 ANGELA T. MELINARAAB, B.F.A., J.D.
 MARGARET M. MENICUCCI, B.A., J.D.
 JO A. MERICA, B.A., J.D.
 RANELLE M. MERONEY, B.A., J.D.
 DARYL L. MOORE, B.A., M.L.A., J.D.
 STEVEN A. MOORE, B.A., Ph.D.
 EDWIN G. MORRIS, B.S., J.D.
 MARCO M. MUNOZ, LL.B., M.C.J.
 MANUEL H. NEWBURGER, B.A., J.D.
 STEVEN P. NICHOLS, B.S.M.E., M.S.M.E., J.D., Ph.D.
 JANE A. O'CONNELL, B.A., J.D.
 PATRICK L. O'DANIEL, B.B.A., J.D.
 GUILLERMO A. PADILLA, J.D., Ph.D.
 M. A. PAYAN, B.A., J.D.
 MARK L. PERLMUTTER, B.S., J.D.
 LOUIS T. PIRKEY, B.S.Ch.E., J.D.
 JUDGE ROBERT L. PITMAN, B.S., J.D.
 ELIZA T. PLATTS-MILLS, B.A., J.D.
 LAURA L. PRATHER, B.B.A., J.D.
 JONATHAN PRATTER, B.A., M.L.S., J.D.
 VELVA L. PRICE, B.A., J.D.
 BRIAN C. RIDER, B.A., J.D.
 GRETCHEN RITTER, B.S., Ph.D.
 ROBERT M. ROACH, JR., B.A., J.D.
 BRIAN J. ROARK, B.A., J.D.
 BETTY E. RODRIGUEZ, B.S.W., J.D.
 JAMES D. ROWE, B.A., J.D.
 MATTHEW C. RYAN, B.A., J.D.
 KAREN R. SAGE, B.A., J.D.
 MARK A. SANTOS, B.A., J.D.
 CHRISTOPHE H. SAPSTEAD, B.A., J.D.
 SUSAN SCHULTZ, B.S., J.D.
 WILLIAM F. STUTTS, B.A., J.D.
 MATTHEW J. SULLIVAN, B.S., J.D.
 GRETCHEN S. SWEEN, B.A., M.A., Ph.D., J.D.
 BRADLEY P. TEMPLE, B.A., J.D.

RICHARD J. SEGURA, JR., B.A., J.D.
JUDGE ERIC M. SHEPPERD, B.A., J.D.
RONALD J. SIEVERT, B.A., J.D.
AMBROSIO A. SILVA, B.S., J.D.
LOUISE SINGLE, B.S., M.T.A., Ph.D.
BEA A. SMITH, B.A., M.A., J.D.
CORY W. SMITH, B.A., J.D.
DWAYNE W. SMITH, B.A., J.D.
TARA A. SMITH, Ph.D.
LYDIA N. SOLIZ, B.B.A., J.D.
JUSTICE ROSE B. SPECTOR, B.A., J.D.
LEWIS J. SPELLMAN, B.B.A., M.B.A., M.A., Ph.D.
DAVID B. SPENCE, B.A., J.D., M.A., Ph.D.
WILLIAM J. SPENCER, B.A., M.S., Ph.D.
LAURA L. STEIN, B.A., M.A., Ph.D.
JAMES B. STEINBERG, B.A., J.D.
PAUL J. STEKLER, Ph.D.
CHARLES H. STILL, B.B.A., J.D.

SHERINE E. THOMAS, B.A., J.D.
TERRY O. TOTTENHAM, B.S., LL.M., J.D.
JEFFREY K. TULIS, B.A., M.A., Ph.D.
ROBERT W. TURNER, B.A., LL.B.
TIMOTHY J. TYLER, B.A., J.D.
VALERIE L. TYLER, B.J., J.D.
SUSAN S. VANCE, B.B.A., J.D.
LANA K. VARNEY, B.J., J.D.
CLARK C. WATTS, B.A., M.D., M.A., M.S., J.D.
JANE M. WEBRE, B.A., J.D.
RANDALL B. WILHITE, B.B.A., J.D.
DAVID G. WILLE, B.S.E.E., M.S.E.E., J.D.
MARK B. WILSON, B.A., M.A., J.D.
JUDGE PAUL L. WOMACK, B.S., J.D.
NOLAN L. WRIGHT, B.A., M.A., M.L.I.S., J.D.
LARRY F. YORK, B.B.A., LL.B.
DANIEL J. YOUNG, B.A., J.D.

VISITING PROFESSORS

ANTONIO H. BENJAMIN, LL.B., LL.M.
PETER F. CANE, B.A., LL.B., D.C.L.
DAVID ENOCH, LL.B., Ph.D.

IAN P. FARRELL, B.A., LL.B., M.A., LL.M.
VICTOR FERRERES, J.D., LL.M., J.S.D.
FRANCESCO FRANCONI, J.D., LL.M.

Texas Law Review

Volume 88

Number 7

June 2010

BRICE A. WILKINSON
Editor in Chief

KATHERINE L.I. HACKER
Managing Editor

J. BENJAMIN BIRELEY
Chief Articles Editor

NICK S. DHESI
Administrative Editor

JAMES I. HUGHES
Chief Notes Editor

GUHA KRISHNAMURTHI
Book Review Editor

NICHOLAS A. JACKSON
Online Content Editor

DANIEL J. AGUILAR
Research Editor

J. MARK LITTLE
SHANE A. PENNINGTON
LAURA E. PETERSON
COLIN C. POGGE
Articles Editors

DANIEL H. COHEN
ROBERT C. DOLEHIDE
JESSICA H. MILLER
Notes Editors

PATRICK T. SCHMIDT
DAVID D. SHANK
MICHAEL J. STEPHAN
TRAVIS R. WIMBERLY
Articles Editors

CHRISTIE M. ALCALA
GREGORY R. BADEN
TYLER J. BEXLEY
WYATT J. DOWLING

KAREN E. FRANCIS
NOAM B. GREENSPAN
DENNIS R. KIHM
JOSEPH A. MAGLILOLO
REX A. MANN
Associate Editors

BILLY JOE McLAIN
HOLLY E. ROBBINS
BRETT J. THOMPSEN
ADAM E. WINSHIP

Members

CEDRIC L. ALLEN
SHANE C. ANDERSON
ANTHONY F. ARGUIJO
TRACEY A. BAMBERGER
LAUREN E. BARROWS
JONATHAN L. CHALTAIN
JOHN CHEN

JONAH D. JACKSON
MICHELLE J. JACOBSON
DON J. KAHN
MICAH R. KEGLEY
W. LAWSON KONVALINKA
ANDREW B. LANGWORTHY

AMELIA C. RENDEIRO
ALICIA R. RINGUET
MICHAEL J. RITTER
ELIZABETH C. ROWLAND
JOHN P. SALMON

SARAH E. COBLE
NEAL A. COLEMAN
SERINE R. CONSOLINO
LAUREN D. CORBEIL
MICHAEL A. CUMMING
STEPHANIE N. DeBROW
KATHERINE N. DOORLEY
ANDREW M. EDGE
ANDREA L. FAIR
JAMIE E. FRANCE
CHRISTOPHER G. GRANAGHAN
CHRISTOPHER T. GRIFFITH
MATT HARDING
JAMES R. HOLCOMB IV
CHRISTOPHER G. HORNIG
SARAH A. HUNGER

DANIEL LENHOFF
ERIC M. LEVENTHAL
JEFFREY LIANG
JAMES R. LLOYD
CLAYTON MATHESON
KATHLEEN M. McCABE
BLAIR K. McCARTNEY
GRAYSON E. MCDANIEL
MYRIAH J. MELTON
ADAM D. MOSES
DENTON P. NICHOLS
OMAR A. OCHOA
ZACHARY T. PADGETT
MICHAEL R. PARKER
MICHAEL P. PARMERLEE
JON REIDY

BRANDON B. SCHUBERT
STEPHANIE N. SIVINSKI
DAVID A. SNYDER
DAWN L. STEINHOFF
JOHN F. SUMMERS
AMANDA M. SUZUKI
ARIELLE B. SWARTZ
CHRISTINE M. TAMER
KRIS Y. TENG
REID A. TEPFER
MARK J. TINDALL
GEORGE D. VALLAS
CATHERINE E. WAGNER
JEFFREY M. WHITE
MARK F. WILES
J. T. WILLIAMS
KRISTEN A. WONG
ALLISON J. ZABY

PAUL N. GOLDMAN
Business Manager

MITCHELL N. BERMAN
JOHN S. DZIENKOWSKI
Faculty Advisors

TERI GAUS
Editorial Assistant

Texas Law Review

Volume 88, Number 7, June 2010

SYMPOSIUM:

LAW AT THE INTERSECTION OF NATIONAL SECURITY,
PRIVACY, AND TECHNOLOGY

I. ACCOUNTABILITY MECHANISMS

- It Came from Beneath the Twilight Zone: Wiretapping and
Article II Imperialism
Heidi Kitrosser 1401
- Deputizing Homeland Security
Jon D. Michaels 1435
- The Case for Stewart over Harlan on 24/7 Physical
Surveillance
Afsheen John Radsan 1475
- Terrorism Trials and the Article III Courts After *Abu Ali*
Stephen I. Vladeck 1501

II. CYBERSECURITY AND NETWORK OPERATIONS

- Cyber Warfare and Precautions Against the Effects of Attacks
Eric Talbot Jensen 1533
- Sovereign Discourse on Cyber Conflict Under International
Law
Sean Kanuck 1571

III. FOCUS ON FISA

- In re Directives Pursuant to Section 105B of the Foreign
Intelligence Surveillance Act: Judicial Recognition of Certain
Warrantless Foreign Intelligence Surveillance
Matthew A. Anzaldi & Jonathan W. Gannon 1599

Programmatic Surveillance and FISA: Of Needles in Haystacks
William C. Banks 1633

IV. INVESTIGATIONS

The Modest Role of the Warrant Clause in National Security
Investigations
Orin S. Kerr 1669

The Argument Against Technology-Neutral Surveillance Laws
Paul Ohm 1685

The Law of Homegrown (Counter)Terrorism
Samuel J. Rascoff 1715

V. NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY

Choosing Both: Making Technology Choices at the
Intersections of Privacy and Security
Alexander W. Joel 1751

The Key Theory: Authenticating Decrypted Information in
Litigation While Protecting Sensitive Sources and Methods
Nicholas J. Patterson 1767

Mending Walls: Information Sharing After the USA PATRIOT
Act
Nathan Alexander Sales 1795

The Right to Privacy in Light of Presidents' Programs: What
Project MINARET's Admissions Reveal about Modern
Surveillance of Americans
Lisa Graves 1855

Texas Law Review

Volume 88, Number 7, June 2010

Symposium

It Came from Beneath the Twilight Zone: Wiretapping and Article II Imperialism

Heidi Kitrosser*

I. Introduction

The past few decades have seen the rise of a deeply influential strain of constitutional argument, sometimes called “presidential exclusivity.” Exclusivists argue that the President has substantial discretion to override statutory limits that he believes interfere with his ability to protect national security.¹ To borrow terminology from Justice Jackson’s famous concurring opinion in *Youngstown Sheet & Tube Co. v. Sawyer*,² exclusivists deem any number of “zone three” presidential actions defensible. On the spectrum of presidential actions, zone three comprises those acts that contravene statutory mandates.³ “Zone one,” in contrast, includes presidential actions that are statutorily authorized.⁴ Presidential actions in “zone two,” or the “zone of twilight,” occur in the absence of legislation either authorizing or prohibiting them.⁵

Exclusivists deem the President’s discretion to act in zone three essential to his constitutional role. In this respect, some emphasize that

* Associate Professor, University of Minnesota Law School. I thank Bobby Chesney for inviting me to participate in the symposium for which I wrote this paper. I also thank the Texas Law Review students and the symposium participants, especially my co-panelists, Jon Michaels, John Radsan, and Steve Vladeck, and panel moderator Sandy Levinson for an outstanding event. Finally, I am grateful to Larry Solum for very thoughtful comments.

1. See, e.g., David J. Barron & Martin S. Lederman, *The Commander in Chief at the Lowest Ebb—A Constitutional History*, 121 HARV. L. REV. 941, 1027 (2008) [hereinafter Barron & Lederman II] (invoking the term “presidential exclusivity” to describe this school of thought); David J. Barron & Martin S. Lederman, *The Commander in Chief at the Lowest Ebb—Framing the Problem, Doctrine, and Original Understanding*, 121 HARV. L. REV. 689, 694 (2008) [hereinafter Barron & Lederman I] (describing exclusivist reasoning).

2. 343 U.S. 579, 634 (1952) (Jackson, J., concurring).

3. *Id.* at 637.

4. *Id.* at 635.

5. *Id.* at 637.

Article II of the Constitution vests “[t]he executive Power” in the President.⁶ Others stress the President’s role as Commander in Chief of the military.⁷ Exclusivists argue that Founding Era understandings and logic dictate that the President, to fulfill these constitutional roles, has significant discretion to violate statutes as he deems necessary to protect national security.⁸ Central to this argument is the premise that the Executive and Commander in Chief powers demand—and the founders structured the Presidency to ensure—the capacity to act with “energy,” meaning with “decision, activity, secrecy, and dispatch”⁹ Statutes that restrict the President’s ability to exercise this capacity to protect national security raise serious constitutional questions, say exclusivists.¹⁰

Exclusivists commonly buttress these arguments by citing American history beyond the founding. For example, when presidential intelligence-gathering operations have been challenged as exceeding statutory limits, exclusivists have defended them by citing to comparable programs throughout American history.¹¹ Non-exclusivists, or “balancers,” typically respond to such arguments by challenging the similarity of the historical examples to current situations or by noting that multiple illegalities do not cancel one another out.¹²

6. U.S. CONST. art. II, § 1, cl. 1; *see also, e.g.*, Gary Lawson, *What Lurks Beneath: NSA Surveillance and Executive Power*, 88 B.U. L. REV. 375, 376, 381–84, 389–93 (2008) (presenting the exclusivist component of his Vesting Clause argument tentatively, explaining that he offers only “a few tentative words on the subject”).

7. *See, e.g.*, U.S. DEP’T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 6–7, 29–35 (2006) [hereinafter DOJ WHITEPAPER] (positing an exclusivist argument by reference to the Commander in Chief Clause); JOHN YOO, *WAR BY OTHER MEANS* 103, 114, 119–22 (2006) (describing justifications for wartime exclusivity grounded partly in the Commander in Chief clause). Of course, the Commander in Chief argument is not exclusive of the Vesting Clause argument. *See, e.g.*, Lawson, *supra* note 6, at 384 (“[A]lthough the [DOJ WHITEPAPER] does not articulate the Vesting Clause thesis with clarity, it seems clear that the Vesting Clause thesis lurks beneath the argument and provides it with substance.”); YOO, *supra*, at 103 (combining Vesting Clause and Commander in Chief arguments).

8. *See, e.g.*, YOO, *supra* note 7, at 119–21 (citing Hamilton’s views in the *Federalist Papers* to support his argument that the President’s discretion to use military powers in national emergencies must not be limited by Congress).

9. Minority Report, *in* REPORT OF THE CONGRESSIONAL COMMITTEES INVESTIGATING THE IRAN-CONTRA AFFAIR, H.R. REP. NO. 100-433, S. REP. NO. 100-216, at 460 (1987) [hereinafter Minority Report] (quoting THE FEDERALIST NO. 70, at 424 (Alexander Hamilton) (Clinton Rossiter ed., 1961)).

10. *See, e.g., id.* (citing Federalist No. 70 to argue that the Constitution gives the President—who is “more energetic” and more politically accountable—control over national security and foreign policy); YOO, *supra* note 7, at 120–21 (citing Federalist No. 70 to argue that the presidential power to protect the nation “ought to exist without limitation”).

11. *See, e.g.*, DOJ WHITEPAPER, *supra* note 7, at 6–8 (chronicling uses of warrantless searches and surveillance under Presidents Roosevelt, Truman, and Johnson).

12. *See, e.g.*, Letter from Curtis A. Bradley et al., to Members of Congress 5–6 (Feb. 2, 2006) [hereinafter Law Professors Letter] (arguing that the long wiretapping history cited by the Bush Administration is irrelevant to current debates because that history predated statutory regulation of wiretapping).

Some commentators chide exclusivists and balancers alike for citing evolving history. For example, Professor Paulsen observes:

Under one school of thought, ours is a “living Constitution,” the meaning of which changes with the times. Under another, the Constitution sets forth immutable principles of fundamental law that must never be altered by mere government officials. The “Living Constitution” position is usually associated with “liberal” constitutional theorists, and the “Original Meaning” position with “conservatives.” But in the area of war powers, the positions of the contending parties seem almost exactly reversed. “Conservatives” frequently defend broad presidential war-initiating power, against the greater weight of evidence of original meaning and design. More shockingly yet, they do so largely for *policy* reasons and defend such antioriginalist constitutional revisionism on the basis of consistent modern *practice*—a position that few conservative constitutional scholars would defend in other areas (like criminal procedure, abortion, or expansive conceptions of federal government power). But so too do “liberals” change their constitutional stripes when it comes to war: In few, if any, areas do those who otherwise so fervently defend the idea of an evolving, changing Constitution cling so tenaciously to the Framers and the original meaning of the words of the Constitution!¹³

Yet unless one rejects the notion that post-founding history can ever shed light on constitutional law, the question is not whether post-founding history categorically is or is not relevant. Rather, the question is case specific: whether—given the constitutional provisions at issue, the post-founding history cited, and the interpretive proposition for which that history is offered—the history indeed furthers the proposition. If one reads the relevant provisions of Articles I and II as sufficiently vague to leave room for bounded shifts in application,¹⁴ then it is important to examine exclusivist uses of evolving history on their own terms. Only then can one determine if evolving historical practice remains within acceptable bounds of constitutional construction and what further light, if any, practice sheds on such construction.¹⁵ Furthermore, as a practical matter, the increasing influence of

13. Michael Stokes Paulsen, *The War Power*, 33 HARV. J.L. & PUB. POL’Y 113, 120 (2010).

14. See Lawrence B. Solum, *Semantic Originalism* 69 (Ill. Coll. of Law, Working Paper No. 07-24, 2008), available at <http://papers.ssrn.com/abstract=1120244> (positing that “constitutional construction operates after interpretation yields semantic content that is vague, ambiguous, or contains gaps or contradictions”).

15. See *id.* at 59 (explaining that “individual words and phrases that comprise the constitution could have different meanings if they were uttered in different contexts”); cf. Jack M. Balkin, *Original Meaning and Constitutional Redemption*, 24 CONST. COMMENT. 427, 433 (2007) (“If the original meaning of the text requires ‘equal protection,’ then we enforce equal protection today because the text continues to require it How we apply the principles of equal protection, however, may well be different from what people expected in 1868 based in part on our contemporary understandings.”).

exclusivity in the political branches and courts alike provides an important independent reason to address major exclusivist arguments, including those from evolving history.

This Article considers exclusivist arguments from evolving history. It finds that such arguments reflect a fundamental error that runs throughout exclusivist analyses. That is, exclusivists conflate the President's structural capacities—in particular, his “energy,”¹⁶—with a legal prerogative to utilize those capacities as he sees fit, even to circumvent statutory constraints, to protect the nation. Elsewhere, I have discussed this error as a matter of text, structure, and Founding Era history. Using these tools, I explain that the President's capacities are constitutionally subject to statutory restraint outside of extraordinary and temporally limited cases, such as where Congress is physically unable to amend legislation in time to confront an emergency.¹⁷ In this Article, I examine this exclusivist error through the use of evolving American history.

This Article focuses predominantly on examples involving wiretapping from the administration of FDR through the present. It identifies two major respects in which exclusivist arguments from evolving history err by conflating capacity with legal prerogative. First, exclusivists deem past instances of presidential initiative or legislative acquiescence (with the latter demonstrated either through silence or through failure to react meaningfully where the President circumvents statutory limits) to arise naturally from the President's and Congress's respective capacities and therefore to reflect the proper constitutional order.¹⁸ Hence, to defend a years-long warrantless wiretapping program during the Bush Administration (the Terrorist Surveillance Program, or TSP) that many concluded violated the Foreign Intelligence Surveillance Act (FISA),¹⁹ the Administration argued that many past presidents had engaged in wiretapping on their own initiative.²⁰ At least one Administration supporter argued that FDR had done so in the face of a prohibiting statute.²¹ Yet this history supports the TSP only if one assumes that a capacity to initiate and undertake a warrantless wiretapping program is the same as a legal prerogative to do so in the face of a contrary statute. If the two are not the same, then the fact that prior administrations have har-

16. Minority Report, *supra* note 9, at 460.

17. I have made this point extensively in the context of the President's capacity to keep secrets. See, e.g., Heidi Kitrosser, *Classified Information Leaks and Free Speech*, 2008 U. ILL. L. REV. 881, 896–926. I also make this point with respect to the President's capacities more generally in Heidi Kitrosser, “Macro-Transparency” as *Structural Directive: A Look at the NSA Surveillance Controversy*, 91 MINN. L. REV. 1163, 1167–73 (2007).

18. See *infra* subpart II(A).

19. See John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565, 565 (2007) (noting that both academic and political critics claim that TSP violates FISA).

20. DOJ WHITEPAPER, *supra* note 7, at 7–8, 16–17.

21. YOO, *supra* note 7, at 114–15.

nessed their capacities to take such initiative, possibly in the face of contrary legislation, hardly proves that such actions are legal prerogatives of the President. If one's premise is that constitutional text, structure, and history dictate that presidential capacities are dangerous and thus to be restrained through legislation, such past instances are better read as cautionary prods to the people and the Congress—reminders of James Madison's warning that the Constitution's "parchment barriers" are meaningless if not actively guarded.²²

Second, another thread in the exclusivist narrative about post-founding history—that past instances of presidential initiative and congressional acquiescence reflect longstanding acknowledgment by each branch of the President's exclusive role in much of foreign affairs and national security²³—is infused with the assumption that acts or omissions reflecting the branches' respective capacities, including the relative ease of unilateral action on the President's part and the difficulty of enacting legislation, also reflect their respective legal prerogatives. This assumption is belied by substantial evidence to the contrary. In the case of wiretapping, for example, while members of the FDR through Kennedy Administrations acknowledged that they wiretapped and at times lobbied Congress for legislation "clarifying" their authority to do so,²⁴ there is a near absence (with one exception discussed below) in the extensive legislative hearings on wiretapping and in administration statements of anything resembling an exclusivist argument.²⁵ To the contrary, these discussions and statements overwhelmingly assume that Congress, even in the midst of a World War, has the legal power to prohibit or restrict national security wiretapping.²⁶

The Article also observes exclusivity's rise over the past several decades. Exclusivity reared its head to a limited degree in congressional hearings preceding FISA's passage in the mid-to-late 1970s.²⁷ By the early twenty-first century, exclusivist arguments were a substantial presence in hearings preceding the 2008 FISA Amendments Act.²⁸ This trajectory reflects the rising influence of exclusivist thought in modern political debate. Exclusivists have themselves become part of the story of the imperial presidency. As their arguments have increasingly entered the mainstream, they have helped to translate the President's structural capacities into legal prerogatives. Indeed, exclusivity has increasingly gained a presence in public debate as well as in the halls of Congress and the courts. Furthermore, by exclusivity's own logic, these developments have an ongoing ratcheting

22. THE FEDERALIST NO. 48, at 308 (James Madison) (Clinton Rossiter ed., 1961).

23. See *infra* subpart II(B).

24. See *infra* notes 74–76, 137–41 and accompanying text.

25. See *infra* note 147 and accompanying text.

26. See *infra* subpart III(B).

27. See *infra* subpart IV(A).

28. See *infra* subpart IV(B).

effect. From an exclusivist perspective, the more that Congress and the President evince respect for exclusivity, the more constitutionally imperative it becomes.²⁹

Part II explains that presidential exclusivity conflates the President's structural capacities with legal prerogatives. This error manifests itself in exclusivist uses of evolving history generally and with respect to wiretapping in particular. Part III examines political-branch developments concerning wiretapping from the FDR through Johnson Administrations. The events demonstrate the President's formidable structural capacities to act despite congressional and public disapproval. The notion that these events bolster exclusivity makes sense only if one assumes that strong presidential capacities must reflect strong legal prerogatives. Instead, the events confirm the wisdom of ringing the President's capacities with statutory limits and inter-branch oversight. Part III also demonstrates the near absence of exclusivity from the political-branch debates over wiretapping during this time. Part IV explains that wiretapping-related exclusivity arguments have begun to gain acceptance and momentum in the political branches over the past few decades. Exclusivists thus have themselves become part of the evolving history that they cite on behalf of their views.

II. Presidential Exclusivity and the TSP

As is now well known, the Bush Administration operated the TSP in secret from shortly after September 11, 2001 until the *New York Times* publicly revealed the program in December 2005.³⁰ Under the TSP, the Administration authorized the National Security Agency (NSA) to wiretap certain calls between the United States and abroad without warrants, despite FISA's prohibition on warrantless wiretapping of calls between the United States and other nations.³¹ As such, TSP critics said that the program took place in zone three and that there was no emergency or other rationale that could constitutionally justify a years-long, secretive statutory violation.³² TSP defenders disputed that it took place in zone three at all. They maintain that FISA was implicitly amended by the joint congressional resolution that authorized the President to use force in the wake of 9/11.³³ In the alternative, they make the presidential exclusivity argument that, if FISA did preclude

29. See *infra* subparts II, IV(B).

30. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

31. *Id.*; OFFICE OF THE INSPECTOR GEN. OF THE DEP'T OF DEFENSE ET AL., REPORT NO. 2009-0113-AS, (U) UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 1 (2009) [hereinafter DOD REPORT], available at <http://www.fas.org/irp/eprint/psp.pdf>.

32. See, e.g., Law Professors Letter, *supra* note 12, at 2-9 (explaining that the TSP violates FISA and that the Commander in Chief Clause does not authorize the violation).

33. See DOJ WHITEPAPER, *supra* note 7, at 2-3 (deeming the AUMF statutory wiretapping authorization as contemplated by FISA).

the TSP, FISA was unconstitutional as so applied.³⁴ As such, the TSP was legal even if it occurred in zone three.³⁵ At minimum, TSP defenders argue that their statutory interpretation should prevail to avoid the constitutional problem that would exist, from an exclusivity perspective, under a different reading.³⁶

To support their constitutional position, TSP defenders explain that presidents have authorized domestic and international wiretapping for national security purposes “at least since the administration of Franklin Roosevelt in 1940.”³⁷ TSP opponents rejoin that this history is not on point, as the cited events took place prior to FISA and hence in zone two.³⁸ Yet at least one TSP defender argues that Section 605 of the Telecommunications Act of 1934, as interpreted by the Supreme Court in two cases decided in 1937³⁹ and 1939,⁴⁰ prohibited wiretapping.⁴¹ Wiretapping engaged in while that version of the Act controlled thus is precedent, he argues, for wiretapping contrary to FISA.⁴² Two other commentators, in a coauthored piece, similarly say that the FDR Administration wiretapped in violation of the Telecommunications Act, establishing “surprisingly” strong—though ultimately insufficient—precedent for the TSP.⁴³

If evolving history is neither categorically irrelevant to nor determinative of presidential-power issues, then the question is why a history of presidential initiative in the face of statutory restraints or congressional silence bears on the TSP’s legality if the TSP occurred in zone three. TSP defenders, and exclusivists generally, do not always spell out the implications of the evolving history that they cite. Yet we can glean, as a matter of logic, two major arguments as to why evolving history might support exclusivity. Furthermore, as I explain in the next section, exclusivists sometimes invoke these arguments explicitly.

34. *Id.* at 35.

35. *Id.* at 3, 35.

36. *Id.* at 3, 28–35.

37. *Id.* at 7; *see also id.* at 7–8, 16–17 (recounting practices of Roosevelt and subsequent presidents authorizing both wartime and peacetime wiretapping); YOO, *supra* note 7, at 114–15 (contending that, until the enactment of FISA, presidents since FDR had authorized peacetime domestic wiretapping); Neal Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent*, 60 STAN. L. REV. 1023, 1025 (2008) (describing the Bush Administration’s defense of TSP through historical precedents).

38. *See* Law Professor Letter, *supra* note 12, at 5–6 (deeming the precedents cited by the Bush Administration irrelevant because they predated FISA); *see also* Katyal & Caplan, *supra* note 37, at 1025–27 (recounting the view of TSP opponents that the historical precedent cited by the Bush Administration does not support the Administration’s actions).

39. *Nardone v. United States (Nardone I)*, 302 U.S. 379 (1937).

40. *Nardone v. United States (Nardone II)*, 308 U.S. 338 (1939).

41. *See* Yoo, *supra* note 19, at 588 & n.164 (stating that FDR ordered surveillance even though the Supreme Court decision of *Nardone I* interpreted section 605 of the Federal Communications Act of 1934 to prohibit electronic surveillance).

42. YOO, *supra* note 7, at 114–15.

43. Katyal & Caplan, *supra* note 37, at 1024, 1027–29.

A. *History as Reflecting Constitutional Capacities, Hence Prerogatives*

The first exclusivist argument from evolving history was invoked explicitly by Professor Yoo, who drafted memoranda justifying the TSP's legality while in the Department of Justice's Office of Legal Counsel.⁴⁴ In a book chapter justifying the TSP's legality published after he left the Justice Department, Yoo argues that the Constitution grants the President control over intelligence policy "because the office's structure allows it to act with unity, secrecy, and speed."⁴⁵ He also cites "[d]ecades of American constitutional practice" whereby, among other things, "[p]residents have long ordered electronic surveillance without any judicial or congressional participation" and whereby "FDR ordered . . . surveillance even though a Supreme Court decision and a federal statute at the time prohibited" it.⁴⁶ Proceeding from founding intent to constitutional structure to evolving history, he explains that the President has been able to take such actions over time—that is, to "[gain] the leading role in war and national security" because of his office's capacities and hence its "superior ability to take the initiative in response to emergencies."⁴⁷

The same logic was voiced in a classic exposition of exclusivity in the *Minority Report of the Congressional Committees Investigating the Iran-Contra Affair* in 1987. The *Minority Report* was joined by Senators James McClure and Orrin Hatch and by Representatives Dick Cheney, William S. Broomfield, Henry J. Hyde, Jim Courter, Bill McCollum, and Michael DeWine.⁴⁸ Years later, as Vice President under George W. Bush and a key supporter of the TSP, Dick Cheney would point to the *Minority Report*—written partly by David Addington, then a committee staff member and later chief of staff to Vice President Cheney and an architect of the TSP⁴⁹—as embodying his views on presidential power.⁵⁰ The *Minority Report* argues that some of the statutory directives that President Reagan and his subordinates were said to have violated in the Iran-Contra affairs were unconstitutional

44. DOD REPORT, *supra* note 31, at 11. For some background on Professor Yoo's involvement with the TSP, see, for example, *id.* at 10–14.

45. YOO, *supra* note 7, at 114.

46. *Id.* at 121, 114–15.

47. *Id.* at 119.

48. *Minority Report*, *supra* note 9, at 431.

49. See Jane Mayer, *The Hidden Power: A Secret Architect of the War on Terror*, NEW YORKER, July 3, 2006, at 44, 49 (stating that Addington "contributed legal research" to the *Minority Report*); Chitra Ragavan, *Cheney's Guy*, U.S. NEWS AND WORLD REPORT, May 29, 2006, at 32, 35 (noting that Addington "helped write" the *Minority Report*).

50. FREDERICK A.O. SCHWARZ JR. & AZIZ Z. HUQ, UNCHECKED AND UNBALANCED: PRESIDENTIAL POWER IN A TIME OF TERROR 154–55, 159–60, 200 (2008) (quoting Vice President Dick Cheney, Remarks to the Traveling Press (Dec. 20, 2005), <http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051220-9.html>).

infringements that the President was free to ignore.⁵¹ The *Minority Report* cites the founding premises that the President will be capable of ““decision, activity, secrecy, and dispatch”” and that he will be readily accountable for his actions.⁵² From this, the *Minority Report* draws a constitutional presumption that activities that call for such capacities or that involve case-by-case decision making for which a single person can most readily be held to account belong to the President alone.⁵³ Among the activities in this category are “the deployment and use of force (but not declarations of war), together with negotiations, intelligence gathering, and other diplomatic communications (but not treaty ratification).”⁵⁴

The *Minority Report* argues that this founding design has been borne out by actions of the political branches throughout history.⁵⁵ The *Minority Report* cites instances in which the President took unilateral action without seeking congressional approval, including covert operations, intelligence gathering, uses of force, and actions taken pursuant to the President’s interpretation of treaties.⁵⁶ The report deems it unsurprising that presidents have frequently asserted rights to act without congressional sanction. It quotes Gary Schmitt’s observation to the effect that such assertions follow naturally from the President’s structural capacities:

To some extent, the enumerated powers found in Article II are deceiving in that they appear understated. By themselves, they do not explain the particular primacy the presidency has had in the governmental system since 1789. What helps to explain this fact is the presidency’s radically different institutional characteristics, especially its unity of office. Because of its unique features, it enjoys—as the framers largely intended—the capacity of acting with the greatest expedition, secrecy and effective knowledge. As a result, when certain stresses, particularly in the area of foreign affairs, are placed on the nation, it will “naturally” rise to the forefront.⁵⁷

B. *History as Reflecting Acknowledgment of Constitutional Prerogatives*

Another implicit and sometimes explicit exclusivist argument is that a history of presidential initiative and congressional acquiescence reflects acknowledgment of presidential exclusivity by both branches. In his book chapter supporting the TSP, for example, John Yoo characterizes “[d]ecades

51. See *Minority Report*, *supra* note 9, at 450–51 (arguing, for example, that the Boland Amendment was “clearly unconstitutional” to the extent that it prohibited the President or his agents from engaging in diplomatic communications with whatever countries he wished).

52. *Id.* at 460 (quoting THE FEDERALIST NO. 70 (Alexander Hamilton)).

53. *Id.*

54. *Id.*

55. *Id.* at 463–69.

56. *Id.*

57. *Id.* at 465–66 (quoting Gary J. Schmitt, *Jefferson and Executive Power: Revisionism and the “Revolution of 1800”*, 17 PUBLIUS 7, 23 n.29 (1987)).

of American constitutional practice” as “reject[ing] the notion of an omnipotent Congress.”⁵⁸ He goes so far as to characterize TSP opponents, who deemed it impermissible for the President to violate FISA in secret for several years after 9/11, as “want[ing] to overturn American historical practice in favor of a new and untested theory about the wartime powers of the President and Congress.”⁵⁹

This argument fits within a more general exclusivist narrative. The narrative posits that Congress, for the bulk of American history, respected presidential exclusivity and thus passed few statutory constraints in the realms of foreign affairs or national security. It was only in the twentieth century, for a period between the two World Wars and then again—with a vengeance—from the 1970s through today, that Congress broke this pattern.⁶⁰ From this perspective, we are today left with a “fettered Presidency” that stands in sorry contrast to the constitutional plan that Congress acknowledged and respected for nearly two centuries.⁶¹ Many of the essays in a 1989 book titled *The Fettered Presidency*, published by the American Enterprise Institute, make this point.⁶² One essay in the collection argues that early congresses “[appear] to have understood [their] power to ‘make all laws . . . necessary and proper for carrying into execution . . . all other powers’ as mandating that [they] ‘facilitate the exercise of executive power in the realm of foreign affairs.’”⁶³ In contrast, the essay’s authors use the example of congressional oversight of covert action to lament that more recent congresses have overstepped their traditional and constitutional role.⁶⁴ The *Minority Report* is rife with similar sentiments. Referring to the use of force without congressional authorization, for example, the report concludes that, “[u]ntil recently, the Congress did not even question the President’s

58. YOO, *supra* note 7, at 121.

59. *Id.* at 124–25.

60. See, e.g., Gary J. Schmitt & Abram N. Shulsky, *The Theory and Practice of Separation of Powers: The Case of Covert Action* (explaining that congressional oversight was generally very deferential to the President until the mid-1970s), in *THE FETTERED PRESIDENCY: LEGAL CONSTRAINTS ON THE EXECUTIVE BRANCH* 59, 61–65 (L. Gordon Crovitz & Jeremy A. Rabkin eds., 1989); Abraham D. Sofaer, *Separation of Powers and the Use of Force* (deeming the War Powers Resolution a shift from “the historic pattern of separation of powers”), in *THE FETTERED PRESIDENCY*, *supra*, at 18–20; John G. Tower, *Congress Versus the President: The Formulation and Implementation of American Foreign Policy*, 60 *FOREIGN AFF.* 229, 229–30, 234, 242–43 (1981) (observing that after World War II, Congress generally deferred to the President’s judgment on national security and foreign policy but that Congress became more aggressive in the 1970s); cf. Barron & Lederman II, *supra* note 1, at 947 (criticizing this narrative, or “legislative abdication paradigm,” as “severely overdrawn insofar as it purports to describe longstanding practice”).

61. See, e.g., Schmitt & Shulsky, *supra* note 60, at 61–65 (arguing that while recent Congresses have adopted an aggressive oversight posture, Congress historically understood its constitutional role as subordinate to the President in national security matters, and this traditional understanding was consistent with founding views); Sofaer, *supra* note 60, at 20 (deeming the War Powers Resolution to threaten the “planned separation of powers” of the Constitution’s founders).

62. *THE FETTERED PRESIDENCY*, *supra* note 60.

63. Schmitt & Shulsky, *supra* note 60, at 62.

64. *Id.* at 62–65, 71–75.

authority.”⁶⁵ It also observes that, “[f]or the Congresses that had accepted the overt presidential uses of military force summarized [elsewhere in the report], the use of Executive power for . . . covert activities raised no constitutional questions.”⁶⁶ The *Minority Report* explicitly links these examples to the case for presidential exclusivity, concluding that:

[c]ongressional actions to limit the President in [the area of foreign policy] should be reviewed with a considerable degree of skepticism. If they interfere with core presidential foreign policy functions, they should be struck down. Moreover, the lesson of our constitutional history is that doubtful cases should be decided in favor of the President.⁶⁷

III. Lessons from the FDR Through Johnson Administrations

In the context of the TSP, then, exclusivists seem to rely on exclusivity to make three main points, whether explicitly or by implication. First, as a descriptive matter, they characterize the period from FDR until FISA’s passage as one in which presidents freely wiretapped without congressional sanction and possibly in the face of a contrary statute. Second, they suggest that this pattern of presidential initiative and congressional acquiescence reflects the respective constitutional capacities of the two branches. From this, they infer a constitutional prerogative on the President’s part to act in the face of a statutory prohibition. Third, they suggest that Congress’s long history of acquiescence reflects its acknowledgment that it lacks much constitutional power to restrict intelligence gathering.

This Part argues that the history does not support exclusivity but rather demonstrates its fatal flaw—its reliance on conflating capacity with legal prerogative. Subpart A explains that the history confirms the relatively great structural capacities of the Presidential office, an advantage compounded by the growth of both technology and government. This structural advantage does not amount to or support a right to ignore legal restraints on the same. To the contrary, evidence of this advantage confirms the wisdom of subjecting presidential capacities to statutory restrictions. Subpart B explains that Congress’s failure to pass legislation in this period to establish or “clarify” restraints on wiretapping reflects the arduousness of the legislative process relative to the President’s capacities for unilateral action. The failure does not reveal a historical consensus that Congress may not legally restrict intelligence gathering. To the contrary, the debates of the time suggest a widely held assumption that it is for Congress to decide (in tandem with the President’s veto power) whether to limit intelligence gathering.

65. *Minority Report*, *supra* note 9, at 467.

66. *Id.* at 469.

67. *Id.*

A. *The Wisdom of Containing the President's Capacities*

1. *The President as Default Policymaker.*—As noted earlier, some observers characterize wiretapping during the FDR Administration as taking place in zone three.⁶⁸ Specifically, they cite Section 605 of the Telecommunications Act of 1934, which provided that “no person receiving . . . any interstate or foreign communication by wire . . . shall divulge or publish the [same] . . . , except through authorized channels of transmission or reception.”⁶⁹ They also cite two Supreme Court cases from 1937 and 1939 (the “*Nardone* cases,” so called after a defendant in the underlying criminal cases), which they characterize as interpreting Section 605 to prohibit all wiretapping by federal officers.⁷⁰ The *Nardone* cases held that statements tapped on a wire (*Nardone I*) and the fruits of such statements (*Nardone II*) must be excluded as evidence in federal courts.⁷¹

Yet as one set of these commentators observes, FDR and his Justice Department vigorously disputed that Section 605, on its own or through the *Nardone* cases, had this effect. They maintained that Section 605 prohibited only wiretapping and “divulg[ing]” its fruits in an evidentiary or similar context.⁷² Attorney General Jackson explained in a 1941 letter to Congress that he had suspended wiretapping for a short period in 1940 because the *Nardone* evidentiary restrictions limited its usefulness. He made clear, however, the Justice Department’s position that wiretapping is legal:

There is no federal statute that prohibits or punishes wire tapping alone

. . . It is [the divulging of evidence obtained by wiretapping in open court] that court decisions hold to violate the statute [S]ince our use of [wiretapping] would have as its chief purpose the proof of a case against criminals, the practical effect of these decisions is to make wire tapping unavailing to law-enforcement officers For this reason it was discontinued by the Department of Justice.⁷³

68. See *supra* notes 6–10 and accompanying text.

69. 47 U.S.C. § 605(a) (2006).

70. See YOO, *supra* note 7, at 114–15 (citing these authorities to argue that FDR wiretapped in zone three); Katyal & Caplan, *supra* note 37, at 1041–52 (citing these authorities to argue that FDR wiretapped in zone three).

71. *Nardone v. United States (Nardone I)*, 302 U.S. 379, 380–82 (1937); *Nardone v. United States (Nardone II)*, 308 U.S. 338, 339–41 (1939).

72. Katyal & Caplan, *supra* note 37, at 1049–52.

73. *To Authorize Wiretapping: Hearing on H.R. 2266 and H.R. 3099 Before the H. Comm. on the Judiciary, 77th Cong. 18–19* (1941) [hereinafter *To Authorize Wiretapping Hearing*] (statement of Robert H. Jackson, Att’y Gen. of the United States); see also Herbert Brownell, Jr., *The Public Security and Wire Tapping*, 39 CORNELL L.Q. 195, 199 (1954) (explaining that Jackson’s suspension was short-lived—FDR ordered that wiretapping resume later that year).

This position was maintained in subsequent administrations.⁷⁴ Herbert Brownell, President Eisenhower's first Attorney General, stated in a 1954 *Cornell Law Quarterly* article that "except for a short period during 1940, every Attorney General over the last twenty-two years has favored and authorized wiretapping by federal officers Moreover, this policy adhered to by my predecessors has been taken with the full knowledge, consent and approval of Presidents Roosevelt and Truman."⁷⁵ In 1962 Attorney General Robert Kennedy told Congress that, under Section 605, it was legal to wiretap, but not to divulge the acquired information as evidence. He observed that all administrations since FDR's have engaged in limited wiretapping and that "Congress has been advised [as such] each year by the Director of the [FBI]."⁷⁶

Despite these confident public pronouncements, there was widespread dispute within and outside of the Executive Branch about wiretapping's legality under Section 605. Attorney General Jackson later acknowledged that he had temporarily suspended wiretapping because he thought it was illegal.⁷⁷ And many within Congress, the press, and the public reacted with dismay to the fact of FBI wiretapping throughout these years, insisting that it was against the law.⁷⁸ A 1940 resolution of the Senate Interstate Commerce Committee deemed wiretapping illegal in light of Section 605 and the *Nardone* cases, but lamented that it is "not likely to be eschewed by law-enforcement agencies."⁷⁹ It added that wiretapping is "especially dangerous at the present time, because of the recent resurgence of a spy system conducted by Government police."⁸⁰ Twelve years later, a *Columbia Law Review* article observed that, "despite the statutes and judicial decisions which purport to regulate wire tapping, today this practice flourishes as a wide-open operation at the federal, state, municipal, and private levels."⁸¹

74. In fact, this position was maintained by the Justice Department until 1965. CONGR. RESEARCH SERV., THE OMNIBUS CRIME CONTROL AND SAFE STREETS ACT: BACKGROUND AND SUMMARY OF ITS PROVISIONS 17 (1968); SUBCOMM. ON CONSTITUTIONAL RIGHTS., SENATE COMM. ON THE JUDICIARY, WIRETAPPING AND EAVESDROPPING: SUMMARY—REPORT OF HEARINGS 1958–1961, 5–6, 15–16, 18–19 (1962).

75. Brownell, *supra* note 73, at 200.

76. *Wiretapping—The Attorney General's Program—1962: Hearing on S. 2813 Before the S. Comm. on the Judiciary*, 87th Cong. 11 (1962) [hereinafter *1962 Wiretapping Hearing*] (statement of Robert Kennedy, Att'y Gen. of the United States).

77. ROBERT H. JACKSON, THAT MAN: AN INSIDER'S PORTRAIT OF FRANKLIN D. ROOSEVELT 68–69 (2003); see also Brownell, *supra* note 73, at 199 (suggesting that Jackson issued the suspension order because he thought wiretapping illegal); *To Authorize Wiretapping Hearing*, *supra* note 73, at 221–22 (citing a *New York Times* article describing Jackson's actions after *Nardone II*).

78. Katyal & Caplan, *supra* note 37, at 1047 ("By this point, hostility towards wiretapping had been expressed by Congress, affirmed by the Court, and applauded by the media.")

79. S. REP. NO. 76-1304, at 4–5 (1940).

80. *Id.*

81. Alan F. Westin, *The Wire-Tapping Problem: An Analysis and a Legislative Proposal*, 52 COLUM. L. REV. 165, 167 (1952); see also *id.* at 168–69 (alerting the reader to the prevalence of wiretapping by private actors and blaming it on the government's poor example).

The article reported “[t]he general mood of the press . . . [as] one of dissatisfaction with the prevalence of unlimited wire tapping.”⁸²

Consider what it says about the Presidency’s structural advantages that, despite the acknowledged existence and hotly contested legality of administration policies permitting FBI wiretapping, the policies persisted for decades.⁸³ This history reflects the natural capacity of the President and his subordinates to prevail by default, simply by continuing to take a disputed course of action.⁸⁴ As government’s “doer” branch, the Executive has unique access to its human and technological resources.⁸⁵ Unlike Congress, which can draft legislation but lacks the tools to implement it, and the Judiciary, which announces but lacks the means to execute legal rulings, the President’s constitutional tools uniquely equip him for self-propelled action.⁸⁶

Presidential wins by default in the wiretapping realm also reflect how the President’s intrinsic capacity advantages are compounded by the growth of government infrastructure since the nation’s founding. Prior to “World War II and the preparations for it in the late 1930s,” communications surveillance—while engaged in, and sometimes heavily so by the federal government—was not entrenched in permanent government infrastructure.⁸⁷ Rather:

The first century and a half of American democracy was marked by intermittent episodes of internal intelligence gathering. Monitoring dissent, by the federal government at least, was undertaken only in response to a crisis of the moment; with the passing of the crisis, the monitoring ceased, and the federal machinery that supported it was dismantled or retooled for other tasks.⁸⁸

In this period, government called upon a hodgepodge of resources for help in intelligence gathering, including private detective agencies, citizens’ groups,

82. *Id.* at 189.

83. See Brownell, *supra* note 73, at 197–200 (chronicling the debate on legality and the continued use of the policy through the years).

84. See Neal Devins, *Presidential Unilateralism and Political Polarization: Why Today’s Congress Lacks the Will and the Way to Stop Presidential Initiatives*, 45 WILLAMETTE L. REV. 395, 399 (2009) (explaining that, given their “power to execute . . . Presidents often win by default”); Terry M. Moe & William G. Howell, *Unilateral Action and Presidential Power: A Theory*, 29 PRESIDENTIAL STUD. Q. 850, 855–56 (1999) (describing President’s unique structural capacity to “shift the status quo by taking unilateral action”); William P. Marshall, *Eleven Reasons Why Presidential Power Inevitably Expands and Why It Matters*, 88 B.U. L. REV. 505, 518 (2008) (citing the President’s first-mover advantage); Mark Tushnet, *Controlling Executive Power in the War on Terrorism*, 118 HARV. L. REV. 2673, 2677 (2005) (citing the President’s first-mover advantage).

85. See, e.g., Marshall, *supra* note 84, at 511–17 (citing examples of the President’s advantageous access to government resources).

86. Moe & Howell, *supra* note 84, at 860–62, 866–70 (describing the weaknesses of Congress and the Judiciary relative to the President).

87. RICHARD E. MORGAN, *DOMESTIC INTELLIGENCE: MONITORING DISSSENT IN AMERICA* 15–16, 36 (1980).

88. *Id.* at 16.

and personnel from throughout the Executive Branch.⁸⁹ Yet “[w]ith World War II, which marked in so many ways the modernization of the American national government, this distinctly premodern pattern of intermittent public-private efforts was broken, and a permanent, specialized domestic intelligence capacity was institutionalized at the federal level.”⁹⁰

The growth of an intelligence infrastructure equips the Executive Branch with a permanent arsenal of powerful tools.⁹¹ The arsenal adds substance to the structural advantages intrinsic in the President’s “doer” role.⁹² Absent a permanent and continuously funded infrastructure, intelligence gathering is obviously more difficult to achieve without explicit congressional sanction and funding.⁹³ The difficulty is all the greater in the face of an explicit congressional prohibition, making it harder, for example, for the President to allocate funds based on vaguely worded appropriations.⁹⁴ Yet, like the effective creation of a large standing army, the creation of a vast and permanent intelligence infrastructure adds substance to the President’s theoretical capacity to go it alone.⁹⁵

As noted, exclusivists infer from the President’s physical capacity to “go it alone” by wiretapping in zone two or zone three that he has a legal prerogative to do so.⁹⁶ Yet the latter need not follow from the former. To the

89. *Id.* at 22–26. An important caveat to this observation is that institutionalized intelligence apparatus arose in the military during the Civil War and in the FBI’s predecessor, the Bureau of Intelligence (BOI) during the infamous Palmer Raid period after World War I. While these events were important precursors to the modern intelligence bureaucracy, they were also products of their times insofar as the infrastructure in each case was at least partly dismantled for a period—in the case of the Civil War because the war ended, in the case of the Palmer Raids because of the disgrace that they brought to the BOI. *Id.* at 19–21, 27–30; David Williams, *The Bureau of Investigation and its Critics 1919–1921: The Origins of Federal Political Surveillance*, 68 J. AM. HIST. 560, 560–61, 579 (1981). The post-Palmer Raids period is particularly interesting as it seems to mark a gray area between the worlds of interim and permanent intelligence infrastructure—while the BOI formally shut down surveillance operations not directly related to criminal investigations, between 1924 and 1936 it “hired paid informers to collect information on the activities of liberal and radical political and labor organizations.” *Id.* at 560, 578.

90. MORGAN, *supra* note 87, at 16; *see also* GARRY WILLS, BOMB POWER: THE MODERN PRESIDENCY AND THE NATIONAL SECURITY STATE 57, 59–61, 82–83, 98 (explaining that a permanent “national security state” arose after World War II, including a permanent surveillance infrastructure).

91. *See* Marshall, *supra* note 84, at 515–17 (noting that the power of the Executive Branch is heightened by its control of intelligence gathering and other technological and human resources).

92. *Id.*

93. *See, e.g.*, WILLS, *supra* note 90, at 99–102 (explaining that the Constitution seeks to check Executive Branch power through Congress’s control over funding and that aspects of the national security state enable the Executive Branch to circumvent this check).

94. *See, e.g.*, HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION 52–53 (1990) (recounting congressional efforts to curtail military activities through explicit funding restrictions).

95. *See supra* notes 91–92; *see also, e.g.*, KOH, *supra* note 94, at 52–53 (detailing examples of military activities that continued to be funded and supported by the Executive Branch despite congressional prohibitions on such funding and support).

96. *See infra* subpart II(A) (explaining that exclusivists often infer from the President’s demonstrated structural capacity to act without or against statutory authority that he has a legal right to so act).

contrary, the wiretapping history discussed above could be invoked to demonstrate the logic of a constitutional design that accords the President strong capacities but deems their uses legally legitimate only when authorized by Congress (in zone one) or at minimum not prohibited by Congress (not in zone three). As history demonstrates, the absence of legal legitimacy alone is not enough to stop a determined administration.⁹⁷ Yet there are logical and historical bases to believe that the stamp of legal illegitimacy has political and practical deterrent effects.⁹⁸ That potential deterrent weakens considerably where presidents manage not only to engage in self-initiated, even statute-violating activity, but to convince Congress, courts, and most importantly the people, that those acts are legally legitimate. Furthermore, the potentially endless ratcheting effect of this pattern should be obvious. The more that presidents act in zone two or three, the more constitutional such behavior becomes from the exclusivist perspective, hence the fewer deterrents on such behavior in the future.⁹⁹ In short, the exclusivist reading of evolving history's constitutional significance in the realm of wiretapping is far from the best, let alone the only plausible, reading. Rather, such reading appears to rest on a deeply underexamined and ultimately mistaken premise—that capacity equals prerogative in the realm of presidential power.

2. *Secrecy*.—The previous subpart addresses only those aspects of mid-twentieth-century wiretapping policies that were publicly known while in place. Yet the President's capacity to keep secrets is an important part of the story as well. First, the FDR administration initially kept the fact of wiretapping a secret. Second, while the fact of wiretapping eventually became known, FDR and his successors dramatically misrepresented its scope and nature for decades. As this history demonstrates, the President's capacity for secret keeping enables him to dissemble about the existence and scope of programs. This helps presidents to obtain years of congressional "acquiescence" that future presidents can cite as precedent of constitutional magnitude.

As the previous section discussed, the FDR administration acknowledged publicly that it wiretapped.¹⁰⁰ Yet it was not consistently so

97. See *supra* 77–83 and accompanying text (chronicling years of wiretapping by different administrations despite debates over the legality of the practice).

98. See, e.g., ATHAN THEOHARIS, *SPYING ON AMERICANS* 132 (1978) (recounting the effects on the Executive Branch of heightened public concern for the rule of law in the wake of the Vietnam War and Watergate); *Justice Department Bans Wiretapping; Jackson Acts on Hoover Recommendation*, N.Y. TIMES, Mar. 18, 1940, at A1 (reporting that Attorney General Jackson's order banning wiretapping might have been in response to backlash after the practice began becoming public).

99. See Marshall, *supra* note 84, at 510 ("Presidential power inevitably expands because of the way Executive Branch precedent is used to support later exercises of power."); *id.* at 511, 521 (explaining that only presidential uses of power tend to be cited as constitutional precedent, whereas presidential abstentions are often overlooked).

100. See *supra* notes 37, 43 and accompanying text.

forthcoming. While the *Nardone* cases were decided in December 1937 and December 1939, the Administration did not publicly acknowledge that it wiretapped until March 1940, shortly after Robert Jackson became Attorney General.¹⁰¹ In his public statement to this effect, Jackson indicated that he would henceforth suspend wiretapping because, “[u]nder the existing state of the law [wiretapping] cannot be done unless Congress sees fit to modify the existing statutes.”¹⁰² On May 31, 1940, Jackson wrote to Congress. Quoting his earlier lament about the “existing state of the law,” he urged Congress to pass legislation enabling the Justice Department to wiretap in a limited class of cases including kidnapping, extortion, racketeering, and national defense matters such as espionage and sabotage.¹⁰³ Yet while Jackson apparently did suspend the program in March of 1940,¹⁰⁴ it was soon reauthorized pursuant to President Roosevelt’s order of May 21, 1940.¹⁰⁵ While the Justice Department acknowledged by late 1941 that it was again wiretapping,¹⁰⁶ Jackson’s May 31, 1940, plea to Congress and similar Administration statements of the time reflect a short-lived effort to keep the program a secret until new legislation could be procured.¹⁰⁷

Furthermore, while the FDR Administration eventually acknowledged the fact of wiretapping and later administrations followed suit,¹⁰⁸ it is now well-known that administrations wildly misrepresented the scope of their wiretapping activities for decades. Administrations repeatedly explained that they wiretapped under careful procedural controls and only in a very limited class of cases involving a handful of specified crimes including espionage, sabotage, and kidnapping.¹⁰⁹ Attorney General Brownell epitomized the public face taken by administrations when he insisted in a 1954 law review article that “[e]xperience demonstrates that the [FBI] has never abused the

101. See Katyal & Caplan, *supra* note 37, at 1048 (citing the Administration’s March 1940 public acknowledgment and its pledge to ban wiretapping going forward); *Justice Department Bans Wiretapping*, *supra* note 98 (citing Administration’s March 1940 admission and pledge to ban wiretapping from that point on).

102. *Justice Department Bans Wiretapping*, *supra* note 98.

103. *Wiretapping for National Defense: Hearing Before the H. Comm. on the Judiciary*, 76th Cong. 1–2 (1940) (statement of Robert Jackson, Att’y Gen. of the United States).

104. JACKSON, *supra* note 77, at 68.

105. THEOHARIS *supra* note 98, at 98–99.

106. *Biddle Approves FBI Wiretapping*, N.Y. TIMES, Oct. 8, 1941, at A4; see also J. Edgar Hoover, *Rejoinder by Mr. Hoover*, 58 YALE L.J. 422, 422–24 (1949) (providing examples of public acknowledgements by Administration members of wiretapping); Katyal & Caplan, *supra* note 37, at 1056–59 (citing inconsistent public signals from the Administration from early- to mid-1941).

107. See Katyal & Caplan, *supra* note 37, at 1052–54 (describing Jackson’s effort to keep the program a secret).

108. See *supra* subpart III(A).

109. See, e.g., *1962 Wiretapping Hearing*, *supra* note 76, at 11–12 (statement of Robert Kennedy, Att’y Gen. of the United States); THEOHARIS, *supra* note 98, at 102 (citing Justice Department statements that wiretapping is strictly controlled); Brownell, *supra* note 73, at 199–200, 207–08 (claiming that wiretapping has been strictly limited across administrations); Hoover, *supra* note 106, at 424 (asserting that the FBI only conducted surveillance under rigid supervision in cases of extreme emergency).

wiretap authority. Its record of ‘nonpartisan, nonpolitical, tireless and efficient service over the years gives ample assurance that the innocent will not suffer in the process of the Bureau’s alert protection of the Nation’s safety.’”¹¹⁰

Of course, a very different reality came to light in the 1970s. Investigations sparked by Nixon Administration scandals brought to light shocking abuses of wiretapping and of intelligence gathering generally by every administration since that of FDR.¹¹¹ Over the years, these revelations have filled volumes of primary and secondary literature. For example, the report of the Church Committee—the 1970s Senate investigative committee headed by Senator Frank Church and charged with investigating intelligence-community abuses—observed that “[b]y 1938, the FBI was investigating alleged subversive infiltration of: the maritime industry; the steel industry; the coal industry; the clothing, garment, and fur industries; the automobile industry; the newspaper field; educational institutions; organized labor organizations; Negroes; youth groups; Government affairs; and the armed forces.”¹¹²

As this history illustrates, the presidential capacity to act in secret can easily be abused. As with the presidential capacity to self-initiate, past abuses of secrecy by no means clearly support exclusivity. To the contrary, they remind us of the wisdom of subjecting the President’s capacities to statutory limits and interbranch oversight. Secrecy-fueled historical abuses also heighten the folly of equating congressional acquiescence with congressional support for exclusivity. History suggests that such acquiescence is often facilitated in part by Congress’s ignorance about past or ongoing secret activities.¹¹³

3. *Accountability.*—Thus far, I have used terms such as “presidency” and “presidential power” to describe the person, acts, and powers not only of the President but of his advisors and of others within the Executive Branch that act or purport to act under color of presidential authority. This usage is a product of the reality that at any given time there are countless individuals who exercise the presidency’s structural capacities—such as the ability to self-initiate and to do so in relative secrecy—and its claimed legal

110. Brownell, *supra* note 73, at 207.

111. See, e.g., MORGAN, *supra* note 87, at 4–8 (describing how the death of J. Edgar Hoover and the Watergate scandal led to the disclosure of records detailing decades of surveillance by the FBI); KATHRYN S. OLMSTED, CHALLENGING THE SECRET GOVERNMENT 1–2, 11–17, 41–44, 94–99 (1996) (recounting the 1970s investigations that revealed decades of surveillance abuses); THEOHARIS, *supra* note 98, at 9–13 (discussing the 1970s investigations of intelligence activities and the political climate and scandals that helped to generate them).

112. S. REP. NO. 94-755, at 32 (1976).

113. See Katyal & Caplan, *supra* note 37, at 1067–68 (questioning the precedential value of presidential actions taken secretly).

prerogatives.¹¹⁴ As a result, the President may either genuinely not know of acts taken in his name or retain plausible deniability regarding the same.¹¹⁵ This bears on exclusivity in an important respect. As we have seen, a key aspect of exclusivity is its conflation of the President's capacity to act energetically with a legal prerogative to do the same regardless of statutory restrictions. Yet exclusivists frequently bolster this analytical move with assurance that the rule of law will be maintained by the President's political accountability. If Americans are unhappy with how he exercises his power, they can retaliate against him or his political allies at the ballot box.¹¹⁶ Yet such assurances do not measure up to the realities of a sprawling Executive Branch and intelligence infrastructure. The accountability-defeating features of these realities are bolstered by the presidency's structural capacity for secrecy, which can obscure chains of responsibility both during and after an activity or program.

In the case of wiretapping, some striking examples of presidential ignorance involve J. Edgar Hoover's misleading communications to Presidents FDR, Truman, and Eisenhower. With respect to FDR, Hoover apparently encouraged FDR's belief that the latter's wiretapping authorizations did not cover surveillance of "subversive activities."¹¹⁷ Yet unbeknownst to FDR, Hoover ensured that the authorizations were applied to subversive activities very broadly defined.¹¹⁸ To Presidents Truman and Eisenhower, Hoover represented that FDR had authorized subversive-activities surveillance.¹¹⁹ Truman and Eisenhower each approved such

114. See, e.g., Lisa Schultz Bressman & Michael P. Vandenberg, *Inside the Administrative State: A Critical Look at the Practice of Presidential Control*, 105 MICH. L. REV. 47, 49–50, 65–70, 93–94 (2006) (explaining that many players, sometimes with conflicting agendas, exercise "presidential" oversight of agency policy making); Kitrosser, *Classified Information Leaks*, *supra* note 17, at 892–93 (noting that several million government employees and contractors have some form of classification authority).

115. See GARRY WILLS, BOMB POWER: THE MODERN PRESIDENCY AND THE NATIONAL SECURITY STATE 52 (2010) (noting that the concentration of emergency powers in the Executive Branch increases the number of individuals who "say they can speak for the President" and thus provide plausible deniability); Bressman & Vandenberg, *supra* note 114, at 78–84, 93–94 (presenting survey results showing that EPA personnel believe that White House pressure on the EPA comes from different and sometimes competing White House offices and is not visible to the public); Heidi Kitrosser, *The Accountable Executive*, 93 MINN. L. REV. 1741, 1763 (stating that a President can distance himself from unpopular actions and also can be genuinely "out of the loop"); Peter M. Shane, *Political Accountability in a System of Checks and Balances: The Case of Presidential Review of Rulemaking*, 48 ARK. L. REV. 161, 172–73, 207–08 (1995) (criticizing George H.W. Bush's Council on Competitiveness as a vehicle to influence agency regulatory decisions while retaining plausible deniability for the President).

116. See, e.g., Minority Report, *supra* note 9, at 460 (citing the President's political accountability).

117. Katyal & Caplan, *supra* note 37, at 1039.

118. THEOHARIS, *supra* note 98, at 66–76; Katyal & Caplan, *supra* note 37, at 1039; Athan G. Theoharis, *The FBI's Stretching of Presidential Directives, 1936–1953*, 91 POL. SCI. Q. 649, 654–61 (Winter 1976–1977).

119. Theoharis, *supra* note 118, at 652.

surveillance based partly on the misconception that they were reaffirming what FDR had authorized.¹²⁰

History is also rife with examples of the intentional provision for presidential plausible deniability regarding intelligence gathering. For example, Athan Theoharis reports that the Carter Justice Department decided not to prosecute former CIA officials for illegal mail opening on the basis that “executive approval . . . could not be established because, under the practice of ‘plausible deniability’ or ‘presidential deniability,’ no ‘written records [were made] of presidential authorizations of sensitive intelligence-gathering operations.’”¹²¹ In the realm of intelligence gathering, presidents and administration officials long have sought to minimize written directives or otherwise take steps to protect presidential deniability.¹²² The importance of deniability is illustrated by a standoff between President Hoover and President Nixon. Hoover, sensitive to increasing public and congressional skepticism over surveillance activities, sought to avoid personal responsibility for certain programs (including but not limited to certain wiretapping programs) by demanding that the President or the Attorney General sign off on them in writing.¹²³ Not surprisingly, President Nixon refused this request.¹²⁴ Adding a final twist to the uncertain lines of responsibility that this confrontation reflects, the Intelligence Community proceeded to engage in some of the activities on which Nixon had refused to sign off, despite Nixon’s apparent belief that his refusal had been their death knell.¹²⁵

Ironically, then, the blanket of broad secrecy and discretion that exclusivity justifies can help to defeat the accountability that exclusivists trumpet. This lesson pokes additional holes in the notion that a history of presidential initiative or congressional acquiescence supports exclusivity. For one thing, it is not always so clear that acts of “presidential” initiative are acts of the President’s initiative. Furthermore, it often is difficult if not impossible for Congress or others to discern what the President—or others acting under color of presidential power—knew or did and when they knew or did it. The latter reflects the problems in equating congressional acquiescence with a knowing embrace of exclusivity. More so, it undercuts the

120. *Id.* at 649, 661–68, 671–72.

121. THEOHARIS, *supra* note 98, at xiii.

122. *Id.* at xi–xiii; *see also, e.g.*, H.R. REP. NO. 95-1283, at 119 (1978) (dissenting views on H.R. 7308) (“In reviewing the abuses of the past, it can be seen that the method used by senior executive branch officials to try to escape responsibility was by establishing ‘plausible deniability.’”); Simon Chesterman, *Secrets and Lies: Intelligence Activities and the Rule of Law in Times of Crisis*, 28 MICH. J. INT’L L. 553, 566 (2007) (describing origins and more expansive later uses of plausible deniability).

123. THEOHARIS, *supra* note 98, at 19.

124. *Id.* at 30–34 (describing Nixon’s insistence on retaining “plausible deniability” in the face of Hoover’s request for specific authorization).

125. *Id.* at 13–14, 19, 32–39.

notion that accountability counterbalances excesses that might otherwise flow from exclusivity.

B. The Near Absence of Exclusivity in the Debates of the Time

The second major premise underlying exclusivist uses of evolving history is that Congress until recently took a hands-off approach to national security and foreign policy, and that this reflects a traditional acceptance of exclusivity by the political branches.

In an important two-article series, Professors David Barron and Martin Lederman challenge this premise. First, they demonstrate that Congress has repeatedly passed legislation constraining the President's conduct of military campaigns from the Founding Era through the present.¹²⁶ They also demonstrate that presidents almost never made explicit zone three arguments—that is, arguments defending the legality of national security actions taken against statutory authority on the basis of their Commander in Chief or Executive Power—prior to the mid-twentieth century.¹²⁷ This was so even when presidents “confronted problematic restrictions, some of which could not be fully interpreted away and some of which even purported to regulate troop deployments and the actions of troops already deployed.”¹²⁸ Exclusivity thus was relatively silent within the political branches until the mid-twentieth century. This Part examines the sound of that silence as it relates to wiretapping while the Telecommunications Act of 1934 remained in effect.

Secondary accounts reflect that FDR did not argue that he had a constitutional prerogative to wiretap in the face of contrary statutory authority.¹²⁹ Rather, he claimed that wiretapping was not statutorily prohibited in all cases. In his May 21, 1940, directive ordering Attorney General Jackson to reauthorize wiretapping, FDR explained his narrow reading of the Supreme Court's interpretation of the Telecommunications Act of 1934 in the *Nardone* cases, stating, “I am convinced that the Supreme Court never intended any dictum in the particular case which it decided to apply to grave matters involving the defense of the nation.”¹³⁰ Attorneys general in subse-

126. Barron & Lederman I, *supra* note 1, at 693, 696–97, 704–15; Barron & Lederman II, *supra* note 1, at 947–48, 951–52, 996–97, 1009–15, 1027, 1058–59; cf. Barron & Lederman I, *supra* note 1, at 772–86 (noting that actions of the Continental Congress during the Revolutionary War and texts of post-revolution state constitutions reflected the understanding that legislatures could direct details of military campaigns waged by the “commanders-in-chief”).

127. Barron & Lederman I, *supra* note 1, at 697, 718–20, 763–64; Barron & Lederman II, *supra* note 1, at 948–49, 952, 993–94, 999–1004, 1007–09, 1015–16, 1027, 1034–35, 1057–58.

128. Barron & Lederman II, *supra* note 1, at 948.

129. THEOHARIS, *supra* note 98, at 99; see also Barron & Lederman II, *supra* note 1, at 1052 (chronicling near absence of any exclusivity claims by the FDR Administration); Katyal & Caplan, *supra* note 37, at 1049–52 (citing the FDR Administration's arguments, all grounded in statutory interpretation).

130. Katyal & Caplan, *supra* note 37, at 1050 (quoting FDR's memorandum to Jackson).

quent administrations also relied on statutory interpretation claims, which they articulated publicly, to defend wiretapping.¹³¹

That exclusivity was outside the bounds of mainstream legal thought at the time is exemplified by a fascinating exchange in the pages of the *Yale Law Journal* in 1949. FBI Director J. Edgar Hoover wrote a letter to the journal challenging statements made in a December 1948 article about FBI practices.¹³² In his letter, Hoover noted that “the FBI does tap telephones in a very limited type of cases.”¹³³ The authors of the original article called Hoover’s “admission” of wiretapping an “astounding statement” in light of Section 605’s prohibition on intercepting and divulging wiretapped information.¹³⁴ In a rejoinder to the authors’ written response, Hoover explained that he had “never attempted to keep [his] views on this subject a secret,” citing public statements by himself and other administration officials throughout the 1940s.¹³⁵ As was typical of administration statements supporting wiretapping in the mid-twentieth century, Hoover did not even hint at the possibility that the President could legally circumvent statutory constraints. Rather, he reiterated the Administration’s public position that Section 605 prohibited the introduction of wiretap-derived evidence but did not outlaw wiretapping itself.¹³⁶

In congressional hearings on wiretapping during World War II,¹³⁷ the sole invocation of exclusivity that I found by an administration official is a statement by Attorney General Francis Biddle during a 1942 House Judiciary Committee hearing. Biddle explained that he had already “publicly made clear” his position that Section 605 does not prohibit wiretapping.¹³⁸ He added that he believed his views to be consistent with those of his predecessor, former Attorney General Jackson.¹³⁹ Yet, “since there [was] some confusion and some doubt on the matter,” Biddle concluded that it would be “extremely valuable for the Congress to clarify [wiretapping authority] in legislation.”¹⁴⁰ To this, Biddle added his belief that

131. See, e.g., *1962 Wiretapping Hearings*, *supra* note 76, at 12–13 (statement of Robert Kennedy, Att’y Gen. of the United States) (explaining that under then current law, wiretapping in itself, without subsequent disclosure, was not a crime); Brownell, *supra* note 73, at 199–200 (arguing that the Telecommunications Act does not make wiretapping a crime in its own right).

132. Thomas I. Emerson & David M. Helfeld, *Reply By the Authors*, 58 *YALE L.J.* 412, 413 (1949).

133. *Id.* at 413 (quoting Hoover’s letter).

134. *Id.* at 413–15.

135. Hoover, *supra* note 106, at 422–23.

136. *Id.* at 424.

137. See *infra* note 147 for description of the scope of my search of congressional hearings on wiretapping during the World War II period.

138. *Authorizing Wire Tapping in the Prosecution of the War: Hearing on H.R. 283 Before the H. Comm. on the Judiciary, 77th Cong. 2* (1942) [hereinafter *Authorizing Wire Tapping*] (statement of Francis Biddle, Att’y Gen. of the United States).

139. *Id.*

140. *Id.*

Congress perhaps could not, and certainly would not, wish to prevent the President, as Commander in Chief of the Army and Navy, making use, in time of war, of the right to tap wires. I think it is very doubtful, if the Commander in Chief found it was essential as a military matter to do this in wartimes, whether the legislative branch of the Government could interfere with that, and I am certain they would not wish to, even if they could.¹⁴¹

These thoughts, to which Biddle made no further reference in his testimony, comprise an exception that proves the rule of exclusivity's general absence from the legal and political debates of the time. For one thing, Biddle's brief statement sits in relative isolation among his own more copious body of statutory arguments to Congress on wiretapping in both the hearing just cited and his 1941 confirmation hearing before the Senate Judiciary Committee.¹⁴² That body of arguments comprises the standard refrain of the FDR and subsequent administrations: that Section 605 does not prohibit wiretapping, that Congress should nonetheless "clarify" the right to wiretap, and that Congress should pass legislation permitting some wiretap-derived evidence to be introduced in court.¹⁴³

Furthermore, the overall tenor of Biddle's comments on wiretapping legislation strongly reinforces the notion that his exclusivist statement was directed at most to extraordinary cases within a normative constitutional context of legislative control. For example, following his exclusivist remark, Biddle discussed the desirability of legislation to clarify the right to wiretap and to allow the limited introduction of wiretap-derived evidence.¹⁴⁴ He

141. *Id.*

142. *Id.* at 2–4; see also *Hearing on Biddle Nomination Before the S. Judiciary Comm.*, 77th Cong. (1941) [hereinafter *Biddle Nomination*]. Barron and Lederman make a similar finding about Biddle's relationship to exclusivity during his tenure as Attorney General. In their review, they found only one exclusivist remark by Biddle (or by anyone in the FDR administration, for that matter)—a comment made "in an almost offhand manner" during a Supreme Court oral argument about the power to try enemy combatants via military commission. Barron & Lederman II, *supra* note 1, at 1055. Barron and Lederman explain that, while Biddle's remark was unusual for the time and stood out even within his own larger body of arguments, it "nonetheless [stood] as an indication that [exclusivity]" was beginning to make "inroads in the political branches." *Id.* at 1055–56.

143. See, e.g., *Authorizing Wire Tapping*, *supra* note 138, at 2–4 (stating that Section 605 does not prevent wiretapping but that it prohibits the introduction of its fruits into evidence, stressing that legislation should be passed narrowing the right to wiretap and permitting wiretap-derived evidence to be used in court); *Biddle Nomination*, *supra* note 142, at 5–6, 10 (explaining his support for limited wiretapping and his view that Congress should pass a law that permits wiretapping but limits its scope and enables Congress to oversee its use); *1962 Wiretapping Hearings*, *supra* note 76, at 11–13 (statement of Robert Kennedy, Att'y Gen. of the United States) (stating that Section 605 does not prohibit wiretapping but that it prevents wiretap-derived evidence from being introduced in court, urging the passage of legislation to narrow wiretapping's permitted uses and allow the introduction of wiretap-derived evidence); Brownell, *supra* note 73, at 199–203 (citing Biddle's views on the meaning of Section 605 and on the need for new legislation, noting that Biddle's views have been shared by all subsequent Attorney Generals including Brownell).

144. See *Authorizing Wire Tapping*, *supra* note 138, at 3–4 (statement of Francis Biddle, Att'y Gen. of the United States) (recommending passage of House Joint Resolution 283 to clarify the legality of wiretapping and permit the introduction of evidence from wiretaps).

noted that “it puts a much greater control in the Congress if they wish at any time—if they think at any time it has been abused—to withdraw that power.”¹⁴⁵ Similarly, Biddle spoke of the importance of congressional oversight as a tool by which Congress could determine if any legislative wiretapping authority has been abused.¹⁴⁶

Most tellingly, Biddle’s lone statement marked the only clear reference, and certainly the only approving one, to exclusivity in the several congressional hearings held to consider authorizing wiretapping during and shortly prior to America’s entry into World War II.¹⁴⁷ Overall, statements of witnesses and questioners alike in these hearings were premised on the assumption that it is for Congress (in conjunction with the President’s veto power) to decide on the proper scope, if any, of a national security wiretapping power.¹⁴⁸ The apparent foreignness of exclusivist reasoning to most hearing participants is captured in an exchange between Congressman Earl C. Michener of Michigan, who spoke favorably of granting the President statutory authority to wiretap for national security purposes, and a witness from the ACLU who deemed wiretapping, and hence legislative authorization for the same, undesirable. The ACLU witness suggested that it might be less dangerous to liberty for a president to violate a statute in a moment of true emergency than for Congress to formally broaden the President’s statu-

145. *Id.* at 4.

146. See *Biddle Nomination*, *supra* note 142, at 6, 10 (statement of Francis Biddle, Att’y Gen. of the United States) (remarking that any wiretapping should be reported regularly to Congress).

147. According to LexisNexis Congressional, there were several congressional hearings on wiretapping between the start of World War II (including before America’s entry into the War) and the War’s end. Hearings by the Senate Interstate Commerce Committee (ICC) focused predominantly on allegations of state and private wiretapping and did not discuss the President’s power to wiretap in any depth. See generally *Investigation of Alleged Wire Tapping, Part 1: Hearing on S. 224 Before the Subcomm. of the S. Interstate Commerce Comm.*, 76th Cong. (1940); *Investigation of Alleged Wire Tapping, Part 2: Hearing on S. 224 Before the Subcomm. of the S. Interstate Commerce Comm.*, 76th Cong. (1940); *Investigation of Alleged Wire Tapping, Part 3: Hearing on S. 224 Before the Subcomm. of the S. Interstate Commerce Comm.*, 76th Cong. (1941) (focusing on state and private wiretapping, based on a reading of large portions of the transcripts as well as an electronic word search of the transcripts for the terms “president,” “commander,” “chief,” “constitution,” “article ii,” “article 2,” “article two,” “second article,” and “executive power”). The remaining hearings listed by LexisNexis Congressional are more relevant to my focus on the role (or relative lack thereof) of presidential exclusivity in World War II Era congressional hearings on wiretapping. Those hearings are thus my main points of reference. They are *Authorizing Wire Tapping in the Prosecution of the War, Part 1: Hearing on H.J. Res. 283 Before the H. Comm. on the Judiciary*, 77th Cong. (1942) [hereinafter *Authorizing Wire Tapping Part 1*]; *Authorizing Wire Tapping in the Prosecution of the War, Part 2: Hearing on H.J. Res. 283 Before the H. Comm. on the Judiciary*, 77th Cong. (1942) [hereinafter *Authorizing Wire Tapping Part 2*]; *To Authorize Wire Tapping: Hearing on H.R. 2266 and H.R. 3099 Before Subcomm. No. 1 of the H. Comm. on the Judiciary*, 77th Cong. (1941); and *Wire Tapping for National Defense: Hearing on H.J. Res. 553 Before Subcomm. No. 1 of the H. Comm. on the Judiciary*, 76th Cong. (1940). I also refer at points to relevant parts of Francis Biddle’s 1941 confirmation hearing as Attorney General before the Senate Judiciary Committee. *Biddle Nomination*, *supra* note 142.

148. See generally *supra* note 147.

tory powers.¹⁴⁹ Michener expressed shock, asking, “[y]ou believe, then, that the Chief Executive, regardless of the Constitution, should just go and do that which he thinks is best and pay no attention to the Congress or the Constitution?”¹⁵⁰ Suffice it to say, neither Michener, the ACLU witness, nor other participants in or following the exchange suggested that the President could constitutionally override legislation in the name of national security.¹⁵¹

Debates over Section 605 and possible amendments thereto belie the exclusivist premise that Congress’s acquiescence (in this case, its failure for decades to pass legislation clarifying the contours of presidential wiretapping power) reflects its belief that it may not constitutionally constrain the President in the realm of national security. To the contrary, the debates of the time, including congressional hearings directly addressing wartime wiretapping, overwhelmingly evince the assumption that national security wiretapping is a matter for legislative policymaking.¹⁵²

The hearings on wartime wiretapping also indicate that many who opposed amending Section 605 did so because they deemed the murky status quo a lesser evil than legislation clearly granting or expanding presidential wiretapping powers.¹⁵³ Thus, Congress’s failure to pass new legislation during World War II, or for years beyond that,¹⁵⁴ hardly reflects an exclusivist consensus. Further, the fact that presidents continued to wiretap for decades in the face of their controversial statutory interpretations and Congress’s inertia reflects the phenomenon discussed in the previous section: the

149. *See To Authorize Wire Tapping, supra* note 147, at 199 (statement of Osmond Fraenkel, American Civil Liberties Union) (noting with apparent approval that during the Civil War Lincoln acted outside the law, and although emergency circumstances may have justified his actions, Lincoln “did not seek to have the law changed” or to “have a great principle of constitutional government disregarded”).

150. *Id.*

151. In his testimony, the ACLU witness stated,

I regret any deviation from the law, but I say this, just as I would rather have somebody lose his temper occasionally and do a cruel act than have somebody do a cruel act in cold blood. So I say if in a moment of intense crisis it is believed that something has to be done, human nature is such that it will be done and afterward it will be judged.

Id. (statement of Osmond Fraenkel, American Civil Liberties Union)

152. *See supra* notes 129–151 and accompanying text. For additional statements evincing this assumption in the wartime congressional hearings, see, e.g., *To Authorize Wire Tapping, supra* note 147, at 2–5 (statement of Rep. Francis E. Walter, H. Comm. on the Judiciary) (arguing for legislation that would give the power to authorize wiretapping to the courts rather than to the executive department); *id.* at 21–29 (statement of Rep. Sam Hobbs) (contending that Congress should grant to the federal government—“whose sole responsibility is to enforce the laws [Congress] write[s]”—the authority to conduct wiretaps); *id.* at 214–17 (statement of Rep. John H. Coffee) (emphasizing that executive investigative agencies should only be able to exercise the “great power” of wiretapping if Congress gives it to them).

153. *See, e.g., id.* at 204–05 (statement of S.D. Kapelsohn, National Federation for Constitutional Liberties) (opposing the proposed amendment on the ground that wiretapping should not be statutorily authorized unless its proponents can demonstrate why it is necessary).

154. CONG. RESEARCH SERV., *supra* note 74, at 16 (stating in 1968 that “[d]uring the past 40 years numerous bills to authorize limited forms of wiretapping have been considered by Congress but none has ever been enacted”).

President's structural capacity to make policy by default. As we have seen, this phenomenon, too, hardly provides logical support for exclusivity.

IV. Presidential Exclusivity from the Omnibus Crime Act Through Today: A Growing Tool of the Imperial Presidency

A. *The Omnibus Crime Bill Through FISA*

Congress finally elaborated on the law of wiretapping in the Omnibus Crime Control and Safe Streets Act in 1968. The Act permitted the Attorney General or a designated Assistant Attorney General to authorize federal agents to apply for federal court warrants to wiretap in investigating particular crimes.¹⁵⁵ Covered crimes included the national security related offenses of espionage, sabotage, and treason.¹⁵⁶ Section 2511(3) of the Act included a vague reservation of power to the President, resolving that:

Nothing contained [herein] shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national-security information against foreign intelligence activities.

Nor shall anything contained [herein] be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.

From the sparse legislative history, recounted by the Supreme Court in *United States v. United States District Court*,¹⁵⁷ and from the Government's own representations in that case, it appears that both Congress and the Executive Branch interpreted § 2511(3) solely to acknowledge that the President may have Jacksonian zone two powers and to disclaim an intent to override the same through legislation.¹⁵⁸ In short, neither political branch read § 2511(3) as an exclusivist statement denying Congress's constitutional

155. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 216 (codified at 18 U.S.C. § 2516 (2006)).

156. *See id.* § 2516(1)(a).

157. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297 (1972).

158. *Id.* at 303-08 (examining the text and history of the statute and concluding that "nothing in § 2511(3) was intended to expand or to contract or to define whatever presidential surveillance powers existed in matters affecting the national security"); *see id.* at 339 & n.3 (White, J., concurring) (explaining that the Government did not claim that Congress could not constitutionally restrict the President's capacity to wiretap in the domestic bombing case at issue); *id.* at 344 ("The United States concedes that the act of the Attorney General authorizing a warrantless wiretap is subject to judicial review to some extent . . . and it seems improvident to proceed to constitutional questions until it is determined that the Act itself does not bar the interception here in question.").

prerogative to restrict the President's power to engage in national security wiretapping. That exclusivity went unmentioned in the Act's legislative history despite the concept's obvious relationship to the subject matter suggests that exclusivity was simply off the radar of most political and legal thinkers of the time.

The scandals that unfolded a few years after the Act's passage appeared to impact exclusivity's relationship to mainstream discourse in two major ways. On the one hand, the scandals of the Watergate era—including revelations that every administration since that of FDR had dramatically abused wiretapping—likely stunted any near-term chance of mainstream respectability for exclusivity. Yet in the longer run, the controversies of the 1970s invigorated and inspired exclusivists. For example, former Vice President and avid TSA defender Dick Cheney has frequently cited his dismay at post-Watergate restrictions on presidential power, including FISA.¹⁵⁹ This dismay helped to inspire his contributions (in collaboration with another future TSA co-architect, David Addington) to the *Iran Contra Minority Report*, an exclusivist classic.¹⁶⁰ Similar reactions were had elsewhere within government, academia, and think tanks, as exemplified by another work mentioned above, the American Enterprise Institute's collection of essays, *The Fettered Presidency*.¹⁶¹ Exclusivity's nascent presence can be spotted in the legislative record underlying FISA. In the hearing transcripts and committee and conference reports from 1976–1978 that I reviewed,¹⁶² the strongest exclusivist position is staked out by Robert Bork. In a 1978 House Judiciary Committee hearing, Bork concludes that FISA “probably” violates Article II.¹⁶³ With respect to war and foreign affairs, Bork reasons that Congress's powers are constitutionally “confined to the major issues, issues such as whether or not to declare war and how large the armed forces shall

159. SCHWARZ & HUQ, *supra* note 50, at 154–55; Devins, *supra* note 84, at 396, 411–13.

160. See, e.g., SCHWARZ & HUQ, *supra* note 50, at 154–61 (describing Cheney's disapproval of the “erosion of presidential power” and how it influenced his contribution to the Minority Report).

161. See Robert H. Bork, *Foreward* to THE FETTERED PRESIDENCY, *supra* note 60, at ix (noting that the articles contained in the book “demonstrate that the office of the president of the United States has been significantly weakened in recent years”); see also, e.g., Tower, *supra* note 60, at 230 (lamenting the decline of presidential power after the Vietnam War).

162. Using the LexisNexis Congressional Database, I obtained the 1976, 1977, and 1978 congressional hearings held on FISA. While the Judiciary and Intelligence Committees of both chambers held hearings, I read only the Judiciary Committee hearings to keep the project manageable. I thus read and summarized hearings of the House Judiciary Committee from 1976 and 1978 and of the Senate Judiciary Committee from 1976 and 1977. I also read and summarized the Joint Explanatory Report of the Committee of Conference No. 95-1720 (1978); the Senate Intelligence Committee Report No. 95-701 (1978); the House Intelligence Committee Report No. 95-1283 (1978); and the Senate Judiciary Committee Report including Minority Views No. 95-604 (1977).

163. *Foreign Intelligence Surveillance Act: Hearings on H.R. 7308 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 95th Cong. 131 (1978) [hereinafter *FISA Hearings I*].

be.”¹⁶⁴ What Congress may not do is “dictate the President’s tactics” in these areas, such as how the President conducts intelligence surveillance.¹⁶⁵ While Bork’s view received a few nods of support in the hearings,¹⁶⁶ most of those who raised Article II-based objections recognized a significant regulatory and oversight role for Congress. Their concern was the power that FISA accorded the Judiciary to grant or deny intelligence-gathering warrants.¹⁶⁷ Even Bork suggested that Congress could play a robust oversight role to ensure that administrations complied with their internal regulations.¹⁶⁸ Bork also supported subjecting non-compliant administrations to civil or criminal sanctions.¹⁶⁹

Of course, the view that ultimately prevailed was that Congress was well within its power to pass FISA. This view was represented in much of the congressional testimony.¹⁷⁰ For example, Attorney General Edward Levi of the Ford Administration testified that, while there was some core of Presidential power that Congress could not infringe, FISA’s restrictions fell

164. *Id.* at 138.

165. *Id.*

166. See *Foreign Intelligence Surveillance Act of 1976: Hearing on S. 743, S. 1888, and S. 3197 Before the Subcomm. on Criminal Laws and Procedures of the S. Comm. on the Judiciary, 94th Cong. 2 (1976)* [hereinafter *FISA Hearings II*] (statement of Sen. McClellan, Chairman, Subcomm. on Criminal Laws and Procedures) (recounting his judgment at the time of the 1974 hearings that if past presidents had derived the power to wiretap from “the Constitution, no statute could change or alter it” and recalling that “the then Attorney General, Mr. Saxbe, and the FBI Director, Mr. Kelley, expressed the same judgment in their [1974] testimony”).

167. See *FISA Hearings I*, *supra* note 163, at 24–28, 48 (statement of Rep. McClory, Member, U.S. House of Representatives) (opining that statutory regulation and congressional oversight are “entirely appropriate,” although the President has some exclusive powers under Article II; his objection to the bill was its concession of a role for the courts); H.R. REP. NO. 95-1283, pt. 2, at 114–21 (1978) (dissenting views of Reps. Wilson, McClory, Robinson, and Ashbrook on H.R. 7308) (arguing that statutory regulation of the area and congressional oversight are appropriate, but that a judicial role is not appropriate); S. REP. NO. 95-701, at 91–96 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4042–48 (additional views of Sen. Wallop) (contending that the bill improperly checks presidential power through *ex ante* judicial intervention; *ex post* congressional review would be a more constitutionally appropriate check).

168. See *FISA Hearings I*, *supra* note 163, at 131, 144–46 (statement of Robert Bork, former Solicitor General of the United States) (noting that Congress will oversee Executive Branch enforcement of its internal regulations so there is no “need to worry about future administrations just changing [those regulations] without anybody in Congress knowing about them”).

169. *Id.* at 144.

170. See, e.g., *id.* at 3–4, 7–8 (statement of Griffin B. Bell, Att’y Gen. of the United States); *id.* at 158 (statement of Jerry Berman, Legislative Counsel, American Civil Liberties Union); *id.* at 81–83 (statement by Senator Edward Kennedy); *Foreign Intelligence Surveillance Act: Hearings Before the Subcomm. on Courts, Civil Liberties, and Admin. of Justice of the H. Comm. on the Judiciary, 94th Cong. 23–24 (1976)* (statement of Philip A. Lacovera, former Deputy Solicitor General); *id.* at 38–39 (statement of John Shattuck, National Staff Counsel, American Civil Liberties Union); *id.* at 40–41 (statement of Dr. Morton Halperin, Director, Project on National Security and Civil Liberties); *id.* at 61, 69 (statement of William Van Alstyne, Professor, Duke University); *id.* at 75–76 (statement of Louis Henkin, Professor of International Law and Diplomacy, Columbia University); *FISA Hearings II*, *supra* note 166, at 16–20, 23–24 (statement of Edward Levi, Att’y Gen. of the United States).

within an area that Congress could regulate.¹⁷¹ With respect to this area, Levi explained that, even if the President had inherent power to act absent congressional action (in short, to take zone two action), Congress could constitutionally regulate such acts (thus placing contrary activity in zone three).¹⁷² As such, Levi affirmed that his and future administrations would be constitutionally obliged to abide by FISA's terms.¹⁷³ This view was also reflected in the fact that Congress removed a so-called "disclaimer" provision that had appeared in an earlier FISA bill.¹⁷⁴ The disclaimer, similar to that in the 1968 Omnibus Crime Act, had disavowed any intent to "limit the constitutional power of the President to order electronic surveillance" in certain cases "if the facts and circumstances giving rise to such order are beyond" FISA's terms.¹⁷⁵ The disclaimer's defenders, including Levi, had deemed it simply a statement of neutrality as to the President's constitutional powers in areas not covered by FISA.¹⁷⁶ Yet disclaimer opponents—who had expressed concern that it would be invoked as a "blank check" by future administrations¹⁷⁷—carried the day when Congress removed the provision

171. *FISA Hearings II*, *supra* note 166, at 16–20, 23–25 (statement of Edward Levi, Att'y Gen. of the United States).

172. *Id.*

173. *Id.* at 16.

174. *Foreign Intelligence Surveillance Act of 1977: Hearings on S. 1566 Before the Subcomm. on Criminal Laws & Procedures of the S. Judiciary Comm.*, 95th Cong. 14–15 (1977) (statement of Griffin Bell, Att'y Gen. of the United States) (citing the provision's removal approvingly); S. REP. NO. 95-604, at 82–83 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3966 (minority views of Sen. Abourezk) (citing the provision's removal approvingly).

175. *FISA Hearing II*, *supra* note 166, at 134 (quoting S. 3197, 94th Cong. § 2528 (1976)).

176. *See, e.g., Foreign Intelligence Surveillance Act: Hearings Before the Subcomm. on Courts, Civil Liberties, & Admin. of Justice of the H. Comm. on the Judiciary*, 94th Cong. 92 (1976) (statement of Edward H. Levi, Att'y Gen. of the United States) (explaining that the provision "in no way expands or contracts the President's constitutional powers"); *FISA Hearings II*, *supra* note 166, at 17–18, 25 (statement of Edward H. Levi, Att'y Gen. of the United States) (interpreting the provision as a statement of congressional neutrality regarding the scope of the President's powers in areas not covered by FISA).

177. *See, e.g., FISA Hearings II*, *supra* note 166, at 30–31 (statement of Morton H. Halperin, American Civil Liberties Union) (suggesting that the disclaimer "would be read, in fact . . . as going beyond . . . neutrality . . . and, in fact, endorsing the notion that there is a power here to wiretap, without a warrant"); *id.* at 35–36 (statement of John Shattuck, American Civil Liberties Union) ("I think it is a mistake, a very serious and grave mistake for anyone who is considering this bill to think that it is neutral on the point of Presidential powers . . ."); *id.* at 66, 69 (statement of Professor Phillip Heymann, Harvard Law School) (expressing concern that the disclaimer is subject to abuse and stating his preference to eliminate it or at minimum to narrow it substantially); *id.* at 67 (statement of Professor Herman Schwartz, Law School, State University of New York at Buffalo) ("[I]t seems to me that what this disclaimer does is to give the President a virtual blank check, and says Congress agrees that he has a blank check when he is dealing with matters affecting foreign affairs not within the scope of this statute."); *id.* at 69 (statement of Dean Louis H. Pollak, University of Pennsylvania School of Law) ("[I]f the Congress wishes simply to reflect its awareness that there may be a claim of inherent Presidential power, then it should couch a waiver, I believe, not in terms which are open to Professor Schwartz's concern that Congress is in effect acknowledging the constitutional claim"); *id.* at 71, 74–76 (statement of Sen. Nelson) (suggesting that the disclaimer raises concerns similar to that raised by the disclaimer in the Omnibus Crime Act, which the previous Administration had interpreted as a license to "engage in wholesale

and labeled FISA the “exclusive means” to conduct electronic surveillance within its coverage.¹⁷⁸

B. *The FISA Amendments Act of 2008*

As the TSP demonstrates, exclusivity had become an influential presence in political and legal circles by the post-9/11 period. To further illustrate exclusivity’s relative political force today, this section briefly recounts exclusivity’s role in the 2008 congressional debates over the FISA Amendments Act (FAA). Specifically, this section considers exclusivity’s role in debates regarding Title II of the Act, which retroactively immunizes telecommunications providers who cooperated with the TSP from lawsuits, so long as the providers acted upon a written request “from the Attorney General or the head of an element of the Intelligence Community (or the deputy of such person) . . . indicating that the activity was (i) authorized by the President and (ii) determined to be lawful.”¹⁷⁹ In congressional hearings and reports leading up to the FAA’s passage, immunity proponents argued, among other things, that it would be unfair to punish companies that “patriotically cooperated with the Government.”¹⁸⁰ Opponents argued that the telecommunications companies have sophisticated legal staffs who are equipped to determine the legality of government requests.¹⁸¹ They added that telecommunications companies supported FISA in the 1970s because it offered them clear legal guidance.¹⁸² Immunity opponents also argued that

electronic surveillance”); *id.* at 81–83 (statement of Professor Nathan Lewin) (observing that the disclaimer clause in the Omnibus Crime Act “has continued to be relied upon by the Department of Justice and by those representing individuals or Government agents who have engaged in electronic surveillance as a source of statutory or constitutional authority” and that the disclaimer in the proposed legislation would be used in the same manner).

178. S. REP. NO. 95-701, *supra* note 167, at 71–72; S. REP. NO. 95-604, *supra* note 174, at 6–7; *id.* at 83 (minority views of Sen. Abourezk) (praising the Senate Judiciary Committee’s removal of the provision).

179. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 802(a)(4)(B), 122 Stat. 2436, 2468 (to be codified at 50 U.S.C. § 1885a).

180. *Strengthening FISA: Does the Protect America Act Protect Americans’ Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 16 (2007) [hereinafter *Strengthening FISA Hearing*] (statement of J. Michael McConnell, Director of National Intelligence); see also, e.g., *FISA Amendments: How to Protect Americans’ Security and Privacy and Preserve the Rule of Law and Government Accountability: Hearing before the S. Comm. on the Judiciary*, 110th Cong. 17–18 (2007) [hereinafter *FISA Amendments Hearing*] (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice) (supporting immunity from suit for telecommunications companies who, “acting out of a sense of patriotic duty,” cooperated with government investigatory information requests).

181. *FISA Amendments Hearing*, *supra* note 180, at 28 (statement of Sen. Cardin) (noting that the providers are “sophisticated companies,” “large companies with big legal staffs”); *id.* at 36–38 (statement of Sen. Durbin) (suggesting that companies are capable of determining the legitimacy of government requests and noting that one company indeed refused to cooperate with the TSP due to legal concerns).

182. *Id.* at 59–60 (statement of Morton Halperin, Director of U.S. Advocacy, Open Society Institute).

the companies are meant to play a gatekeeper role against government illegality.¹⁸³

Exclusivist arguments helped immunity proponents to prevail in the final legislation in two major respects. First, as evidenced in congressional reports from 2007 and 2008, several members of Congress adopted the view that the TSP was legal from an exclusivist perspective.¹⁸⁴ For example, Senators Bond, Chambliss, Hatch, and Warner criticized “[t]hose who constantly harp on the misleading assertion that the TSP was illegal.”¹⁸⁵ The Senators expressed their belief, “without any doubt, that the President properly used his authority under Article II”¹⁸⁶

Second, the ubiquity of exclusivist arguments in defense of the TSP simply muddied the waters. The arguments’ presence helped some congresspersons and witnesses to justify immunity without taking a clear stance on exclusivity. That is, it enabled them to deem questions about the TSP’s legality terribly complex and possibly irresolvable. As such, they suggested that it would be unwise and unjust to linger on those questions or to allow litigation about them to proceed. For example, former Deputy Assistant Attorney General Patrick Philbin told the Senate Judiciary Committee that it would have been unfair to expect telecommunications companies to examine the legality of presidential requests to cooperate with the TSP.¹⁸⁷ He explained that “the legal questions . . . often involve constitutional questions of separation of powers that have never been squarely addressed by courts, and are not readily susceptible for analysis by lawyers at a company whose primary concern is providing communications services to the public.”¹⁸⁸ Assistant Attorney General for National Security Kenneth Wainstein testified

183. See, e.g., *FISA Amendments Hearing*, *supra* note 180, at 46–47 (statement of Edward Black, President and CEO, Computer and Communications Industry Association) (discussing the need for companies to resist improper government demands for information); *id.* at 50 (statement of Morton H. Halperin, Director of U.S. Advocacy, Open Society Institute) (identifying the importance of the FISA process in guiding companies as to when to comply with government requests for information); *Strengthening FISA Hearing*, *supra* note 180, at 56 (statement of Suzanne E. Spaulding, Principal, Bingham Consulting Group) (“telecommunications providers [must be] our last line of defense against abuse by the government.”); S. REP. NO. 110-258, at 20 (2008) (additional views of Sen. Leahy) (explaining that retroactive immunity “would subvert the gatekeeping role that FISA contemplates for the providers”).

184. S. REP. NO. 110-258, at 36 (minority statements of Sens. Kyl, Hatch, Grassley, Sessions, Graham, Cornyn, Coburn & Brownback) (“Congress cannot take away the President’s power to monitor foreign enemies of the United States without a warrant. . . . To the extent that FISA purports to do so, it is unconstitutional.”); S. REP. NO. 110-209, at 35 (2007) (additional statements of Sens. Bond, Chambliss, Hatch, and Warner) (“Those who constantly harp on the misleading assertion that the TSP was illegal conveniently ignore federal case law that recognizes the President’s Article II authority to engage in warrantless surveillance in the context of gathering foreign intelligence.”).

185. S. REP. NO. 110-209, at 35.

186. *Id.*

187. *FISA Amendments Hearing*, *supra* note 180, at 49 (statement of Patrick F. Philbin, Partner, Kirkland & Ellis).

188. *Id.*

before the same Committee in support of retroactive immunity.¹⁸⁹ Wainstein also opposed Inspector General review of the TSP, deeming it best to “leave that aside in terms of whether the TSP was within the constitutional authority of the President or not, legal or not, and just focus on how we’re going to fix FISA for the American people.”¹⁹⁰

Congressional debate over FAA’s immunity provisions also reflects an exclusivist tendency to blur or stretch the concept of “emergency” to suggest that any number of actions taken over long time periods fall within the President’s emergency prerogatives. This tendency takes the form of arguments that entail four major steps. First, such arguments start from the exclusivist premise that the President has a legal prerogative, at least in some cases, to circumvent statutory limits that interfere with his ability to defend national security. Second, they involve an assumption or explicit explanation to the effect that such prerogatives stem in large part from the fact that the President is the sole constitutional actor who is structurally equipped to respond to emergencies. Third, they categorize a particular challenged action as an “emergency” action that falls within the President’s constitutional prerogatives. Fourth, they take step three even when the action in question occurred long after Congress could feasibly have acted, and when the temporal component of the emergency rationale thus is absent.

This exclusivist approach to emergency is illustrated in a book passage in which John Yoo defends the TSP.¹⁹¹ Yoo explains that the Constitution’s framers “created an executive with its own independent powers to manage foreign affairs and address emergencies which, almost by definition, cannot be addressed by existing laws If ever there were an emergency that Congress could not prepare for, it was the war brought upon us on 9/11.”¹⁹² The problem with this appeal to emergency is that it seeks to justify a program that went on for years. Even if Yoo’s argument could have justified circumventing FISA in the days immediately following 9/11 (putting aside the fact that FISA already provided for its own 15-day suspension in the case of a congressional war declaration),¹⁹³ it hardly follows that the appeal to emergency justifies years of statutory circumvention.

This tendency to stretch the concept of emergency also factored into the congressional debates on retroactive immunity. For example, the Senate Intelligence Committee, in a 2007 report on the FAA, supported immunity based partly on its view that the telecommunications providers had a “good

189. *Id.* at 7 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice) (testifying that “as a matter of fundamental fairness and as a way of ensuring that providers will continue to provide cooperation to our surveillance efforts,” retroactive immunity is necessary).

190. *Id.* at 11.

191. YOO, *supra* note 7, at 119–20

192. *Id.*

193. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 111, 92 Stat. 1783, 1796 (codified at 50 U.S.C. § 1811 (2006)).

faith” belief in the TSP’s legality.¹⁹⁴ To reach this view, the Committee considered, among other things, “the extraordinary nature of the time period following the terrorist attacks of September 11, 2001.”¹⁹⁵ Yet as the Committee noted in the same report, while the providers received initial request or directive letters from the government shortly after 9/11, they received renewed requests or directives “at regular intervals” thereafter.¹⁹⁶ On a note similar to that struck by the Senate Intelligence Committee, Assistant Attorney General Wainstein stressed, in support of immunity, that the government had contacted the providers “in the aftermath of the worst attack upon the United States, at least since Pearl Harbor.”¹⁹⁷ Former Deputy Assistant Attorney General Philbin also testified that “protecting the carriers who allegedly responded to the government’s call for assistance in the wake of the devastating attacks of 9/11 is simply the right thing to do.”¹⁹⁸

V. Conclusion

Exclusivists have been remarkably successful over the past several decades in shepherding exclusivity from a fringe notion to one with widespread mainstream purchase. Americans may still scoff when presented with exclusivity in a form as stark as Richard Nixon’s infamous line, “[W]hen the [P]resident does it, that means that it is not illegal.”¹⁹⁹ Yet precisely this notion underscores politically influential arguments to the effect that the TSP was legal or that its legality is a matter on which reasonable people can disagree. As we have seen, those arguments have had some success in deterring TSP investigations and in shaping related legislation. Such arguments are also used to deter future restrictions that exceed administration preferences. For example, a Justice Department witness told Congress during the 2007 hearings on the FAA that the Bush Administration would not feel the need to invoke exclusivity to circumvent the FAA if it is satisfied with the final legislation.²⁰⁰

There are descriptive lessons to be gleaned from exclusivity’s rise. The history sheds light on important and dynamic relationships between political and legal argument and political and legal legitimacy. It also helps to illumi-

194. S. REP. NO. 110-209, at 10–11 (2007).

195. *Id.*

196. *Id.* at 10.

197. *FISA Amendments Hearing, supra* note 180, at 8 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice).

198. *Id.* at 48 (statement of Patrick F. Philbin, Partner, Kirkland & Ellis, L.L.P.).

199. SCHWARZ & HUQ, *supra* note 50, at 155–56 (quoting Nixon’s exchange with television interviewer David Frost).

200. *FISA Amendments Hearing, supra* note 180, at 15 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice) (remarking that since the President and Congress were moving “toward a point where we are all on the same page . . . there is not going to be any need for the executive branch to go beyond what FISA has required”).

nate the under examined role of constitutional theory in the oft-told story of the imperial presidency.

Normative engagement with exclusivity is called for as well. As we have seen, among exclusivist arguments are those that draw from evolving history. These arguments start from the premise that there is a long history of congressional acquiescence and presidential initiative with respect to national security. This history, exclusivists argue, reflects the correct constitutional order, one in which Congress oversteps when its legislation conflicts with presidential judgments concerning national security and in which presidents may circumvent such legislation.

The first and most important response to this line of exclusivist argument is simply to deconstruct it. That is, to ask why a history of congressional acquiescence and presidential initiative necessarily supports exclusivity. As we have seen, exclusivists sometimes take this point as a given. Second, once we probe more deeply into the history, we may find—as is certainly true in the case of wiretapping—that relative congressional inaction does not reflect anything close to an exclusivist consensus on Congress's part and that even the Executive Branch has not consistently taken an exclusivist stance. Of course, this historical insight does not answer the question of whether, why, and to what extent post-founding political branch history *should* matter in the realm of separated powers. Still, it is an important corrective to the historical narrative often assumed among exclusivists. At minimum, it calls into question the veracity of the notion—for whatever the notion might be worth if true—that critics of programs like the TSP “want to overturn American historical practice in favor of a new and untested theory about the wartime powers of the President and Congress.”²⁰¹

Finally, even where evolving historical arguments reflect some historical truths—such as the fact that administrations from FDR onward wiretapped despite the view of many that wiretapping was illegal under the 1934 Telecommunications Act²⁰²—exclusivity does not follow automatically from the same. To the contrary, historical developments may prove to be so deeply at odds with constitutional principles as to counsel that the historical course be righted, not that the nation throw its hands up in defeat. As we have seen, decades of wiretapping abuses at the highest levels of American government offer just such counsel. What history has yet to reveal is whether we will heed its lessons.

201. YOO, *supra* note 7, at 124.

202. *See supra* subpart III(A).

Deputizing Homeland Security

Jon D. Michaels*

Introduction

In the wake of the attacks of September 11, 2001, private actors have come to occupy a remarkably prominent place in efforts to identify and counter threats of domestic terrorism. Today, seemingly no transaction, whether social, political, or economic, is comfortably beyond eye or earshot of the newly deputized national security apparatchiks. Corporations representing all of the major retail and service industries—including telecommunications, finance, and commercial travel—are routinely turning over reams of information to the government.¹ And, it's not just corporate data dumps; it's also doormen,² pilots,³ truck drivers,⁴ retail clerks,⁵

* Acting Professor of Law, UCLA School of Law. The author thanks Frederic Bloom, Toni Michaels, Paul Schwartz, David Super, Jonathan Zasloff, and Noah Zatz for their helpful comments. Further thanks are owed to his fellow Symposium participants, to Laura Podolsky, Ira Steinberg, and the UCLA Law Library for invaluable research assistance, to the staff of the Texas Law Review, and to Bobby Chesney for his leadership as Symposium organizer and host.

1. See, e.g., Chris Jay Hoofnagle, *Big Brother's Little Helpers: How Choicepoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 621 (2004) (noting increased government outreach to corporations for customer information); JAY STANLEY, *THE SURVEILLANCE-INDUSTRIAL COMPLEX* 10–11 (2004), http://aclu.org/files/FilesPDFs/surveillance_report.pdf (providing examples of corporations sharing data with the government); see also Leslie Cauley & John Diamond, *Telecoms Let NSA Spy on Calls*, USA TODAY, Feb. 6, 2006, at A1 (reporting on telecom companies' role in facilitating government wiretapping of international communications without warrants or court orders); Mark Glassman, *4 More Airlines Named in Release of Data*, N.Y. TIMES, June 24, 2004, at A17 (describing the practice among airlines of turning over passenger information to government contractors); Philip Shenon, *Airline Gave Defense Firm Passenger Files*, N.Y. TIMES, Sept. 20, 2003, at A1 (reporting that JetBlue voluntarily gave the Defense Department information on more than one million of its customers); Mike Snider, *Privacy Advocates Fear Trade-off for Security*, USA TODAY, Sept. 13, 2001, at D8 (describing Internet service providers' cooperation with federal authorities); Becky Yerak, *"Suspicious Activity" Reports Soar from Banks, Other Depositories*, CHI. TRIB., Nov. 23, 2007, at B3 (reporting on commercial institutions' increased filing of "suspicious activity reports" to the U.S. government); Josh Meyer & Greg Miller, *U.S. Secretly Tracks Global Bank Data*, L.A. TIMES, June 23, 2006, at A1 (detailing financial institutions' cooperation with the government in efforts to detect terrorist financing patterns). When referring to the government in this Article, typically it is to the federal government. At times, however, the term government refers to state or local authorities, or some combination of "state actors" at the local, state, and federal level.

2. See Stevenson Swanson, *Truckers, Doormen Vigilant for Threats*, CHI. TRIB., Aug. 2, 2005, at C11 (reporting that thousands of doormen at residential buildings nationwide have received training to detect terrorist threats and encouragement to alert the authorities if they observe suspicious activity).

3. See Ricardo Alonso-Zaldivar, *Pilots Asked To Be Vigilant*, L.A. TIMES, Mar. 4, 2003, at A14 (noting the collaboration between the Transportation Safety Administration and the 500,000-member Aircraft Owners and Pilots Association to detect and report perceived security threats).

repairmen,⁶ and parcel couriers,⁷ who have been enlisted by the government, their employers, and even their own unions to detect and report suspicious activities on the ground. Finally, there is the role being played by ordinary folks, who have been bombarded with calls from government officials to do their part to keep America secure.⁸

Four factors help explain this dramatic rise in citizen and corporate participation: first, a post-9/11 demand for greater surveillance and

4. OFFICE OF INSPECTOR GEN., DEP'T OF HOMELAND SEC., EFFECTIVENESS OF THE FEDERAL TRUCKING INDUSTRY SECURITY GRANT PROGRAM 1 (2008), http://www.dhs.gov/xoig/assets/mgmt/rpts/OIG_08-100_Sep08.pdf; see also Amanda Ripley, *Eyes and Ears of the Nation*, TIME, June 27, 2004, at 38 (describing the private-public Highway Watch program involving truck drivers in counterterrorism surveillance).

5. See, e.g., Josh Meyer, *As Terrorism Plots Evolve, FBI Relies on Agent John Q. Public*, L.A. TIMES, May 12, 2007, at A1 (describing how the Fort Dix terrorist plot was foiled in part by a Circuit City employee alerting the authorities to suspicious materials on a laptop he was servicing).

6. See Larry Atkins, *Beware of Cable Guys Snooping Around the Neighborhood*, CHI. TRIB., July 23, 2002, at N19 (describing the practice of repairmen being enlisted to assist the authorities in reporting on suspicious activities in their customers' homes); Stephanie Erickson, *"Bright Eyes" Keeping Watch in 7 Counties*, ORLANDO SENTINEL, July 21, 2005, at H1 (noting that Bright House technicians "are hooking up cable television lines and checking Internet connections on the fritz—all while keeping an eye out for terrorism"); Stacy Humes-Schulz, *Alarm Bells Ring Over Terrorism Reporting System*, FIN. TIMES, July 23, 2002, at 6 (reporting on the role repairmen and other service technicians, who do their work in clients' homes, would play in the Justice Department's Operation TIPS).

7. See Robert Block, *Private Eyes: In Terrorism Fight, Government Finds a Surprising Ally: FedEx*, WALL ST. J., May 26, 2005, at A1 (detailing FedEx's post-9/11 assistance in counterterrorism efforts).

8. See Associated Press, *Excerpts from Bush's Briefing*, CHI. TRIB., Oct. 12, 2001, at I18 ("The American people, obviously if they see something out of the norm that looks suspicious, they ought to notify local law authorities . . ."); Michael Cabanatuan, *BART Riders Will Be Asked To Stay Alert*, S.F. CHRON., Aug. 30, 2002, at A24 (noting that mass transit users are encouraged to report suspicious activities); John J. Goldman, *Workers Get Anti-terror Lessons*, L.A. TIMES, May 27, 2004, at A26 (noting that the Attorney General and the FBI Director "called on the nation . . . to help find seven suspected al Qaeda operatives and to head off a possible attack in the U.S."); *Passengers Asked To Help Keep Transit Safe*, USA TODAY, July 8, 2005, at A5 (reporting on government efforts to urge public transit users to advise the police if they see suspicious activities or items); *Transcript of News Conference by Ashcroft and Ridge on Increased Alert*, N.Y. TIMES, Sept. 11, 2002, at A12 (encouraging citizens to report suspicious activity).

It is, to be sure, these ordinary folks who have been asked to be vigilant in their neighborhoods and who have also—now on several commercial flights—been the only ones standing between us and, perhaps, a handful of 9/11-like recurrences. See Brian Harmon et al., *Jet Passengers Foil Shoe-Bomb Suspect*, N.Y. DAILY NEWS, Dec. 23, 2001, at 3; Charles Lane et al., *A Sky Filled With Chaos, Uncertainty and True Heroism*, WASH. POST, Sept. 17, 2001, at A3; Scott Shane & Eric Lipton, *Passengers' Actions Thwart a Plan To Down a Jet*, N.Y. TIMES, Dec. 27, 2009, at A1. See generally David Brooks, Op-Ed. Column, *The God that Fails*, N.Y. TIMES, Jan. 1, 2010, at A29.

Brooks, writing in the immediate aftermath of a thwarted attempt to ignite a bomb on a Detroit-bound flight, notes:

At some point, it's worth pointing out that it wasn't the centralized system that stopped terrorism in this instance. As with the shoe bomber, as with the [United 93] plane that went down in Shanksville, Pa., it was decentralized citizen action. The plot was foiled by nonexpert civilians who had the advantage of the concrete information right in front of them—and the spirit to take the initiative.

Id.

intelligence-gathering capacity;⁹ second, a growing comfort with private actors handling sensitive national security tasks;¹⁰ third, a recognition that much of the desired information is easier for private actors to access or acquire in the first place;¹¹ and, fourth, widespread interest on the part of a patriotic, frustrated public to help.¹²

Enter our new cadre of private snoops, data crunchers, and (yes) vigilantes. This assortment of “deputies,” some trained and ostensibly commissioned,¹³ some solicited as part of a general, mass invitation,¹⁴ and some merely self-declared and possibly unwelcomed,¹⁵ have expanded

9. See NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT, at xv–xvi, 339 (2004) [hereinafter 9/11 COMMISSION REPORT] (describing the need to devote greater resources to intelligence gathering); Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post 9/11 World*, 94 CAL. L. REV. 1655, 1655 (2006) (stating that the attacks of September 11 “resulted, at least in part, from a massive breakdown in the intelligence system designed to identify threats to the nation’s security and to provide policymakers with sufficient information to protect against them”); Jon D. Michaels, *All the President’s Spies: Private–Public Intelligence Partnerships in the War on Terror*, 96 CAL. L. REV. 901, 901–02 (2008) (describing the need for greater intelligence-gathering capacities).

10. See, e.g., Jon D. Michaels, *Beyond Accountability: The Constitutional, Democratic, and Strategic Problems with Privatizing War*, 82 WASH. U. L.Q. 1001 (2004) (describing private military firms’ responsibilities in supplementing, complementing, and, at times, standing in for U.S. military personnel in zones of armed engagement); Martha Minow, *Outsourcing Power: How Privatizing Military Efforts Challenges Accountability, Professionalism, and Democracy*, 46 B.C. L. REV. 989, 992–93 (2005) (discussing private contractors’ involvement in U.S. military engagements, surveillance programs, and military-detention operations); PAUL R. VERKUIL, *OUTSOURCING SOVEREIGNTY* 23–42 (2007) (describing private-sector involvement in a range of national security domains); James Risen & Mark Mazzetti, *Blackwater Guards Tied to Secret Raids by C.I.A.*, N.Y. TIMES, Dec. 11, 2009, at A1 (reporting on the role private security guards played in CIA operations in Iraq and Afghanistan).

11. See Michaels, *supra* note 9 at 902 (indicating that the private sector’s “comparative advantage over the government in [data gathering] is a function both of industry’s unparalleled access to the American public’s intimate affairs . . . and of regulatory asymmetries” that at times enable private organizations to “obtain and share information more easily and under fewer legal restrictions than the government can”). For background on data gathering and analysis, see DANIEL J. SOLOVE, *DIGITAL PERSON* (2004); see also *infra* notes 26 and 70. As Solove notes,

Personal information [mined from business databases] can help the government detect fraud, espionage, fugitives, drug distribution rings, and terrorist cells. Information about a person’s financial transactions, purchases, and religious and political beliefs can assist the investigation of suspected criminals and can be used to profile people for more thorough searches at airports.

SOLOVE, *supra*, at 166.

12. See *infra* note 37 and accompanying text.

13. See, e.g., OFFICE OF INSPECTOR GEN., *supra* note 4, at 1 (noting that the Highway Watch program trains and certifies truck drivers to assist in counterterrorism surveillance).

14. See Andy Newman, *Citizen Snoops Wanted (Call Toll-Free)*, N.Y. TIMES, July 21, 2002, at D1; Eileen Sullivan & P. Solomon Banda, *Anti-terror Citizens Watch Endorsed by Police Chiefs*, STAR-LEDGER (Newark, N.J.), Oct. 4, 2009, at 11.

15. For example, the private, border-patrol “militias” might fall into this category of self-appointed deputies, as might the so-called private Internet vigilantes who monitor and seek to disable Jihadist Web sites and chat rooms. For further discussion of these groups, see *infra* notes 124–25.

homeland security coverage in profound ways.¹⁶ Deputies are force multipliers; as a matter of sheer numbers, a mobilized, vigilant public can reach more broadly than the government, on its own, can. The public does so simply by going about its routine social, civic, and commercial activities in a more mindful manner. Additionally, deputies may have superior physical and electronic access to private spaces and stores of data than government agents have on their own—a function both of there sometimes being greater legal constraints imposed on government agents than on private actors¹⁷ and of the greater caution and reserve people typically exercise when they are interacting with the government, as opposed to when they are engaging with neighbors and merchants, or when they are relying on commercial service providers to facilitate their transactions.¹⁸

Notwithstanding the apparent utility of harnessing the private sector for force multiplication and superior access,¹⁹ deputization has changed us—our

16. STANLEY, *supra* note 1, at 2; cf. Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 7 (2008) (describing the “National Surveillance State” and noting that “[i]n the National Surveillance State, the line between public and private modes of surveillance and security has blurred if not vanished. Public and private enterprises are thoroughly intertwined.”).

17. See *infra* section II(B)(4).

18. Some classic Fourth Amendment cases provide support for the rationale that people do not assume—and, at least in this context, aren’t penalized for not assuming—that business relations with access to their personal property will use that access to facilitate criminal investigations. See *Stoner v. California*, 376 U.S. 483, 489 (1964) (holding that hotel managers may not admit police into guests’ rooms absent a warrant); *Chapman v. United States*, 365 U.S. 610, 617 (1961) (holding that a landlord may not grant the police warrantless entry into a tenant’s residence); *United States v. Jeffers*, 342 U.S. 48, 51 (1951) (indicating that a hotel staff had access to a room for purposes of cleaning and maintenance but not the authority to admit police). There is, however, no corresponding Fourth Amendment protection where third parties, such as banks and telecoms, transfer customer data to the government absent the production of a warrant or the customer’s consent. See *Smith v. Maryland*, 442 U.S. 735, 743–45 (1979) (holding that there is no constitutional expectation of privacy that prohibits telecoms from facilitating warrantless government pen registers); *United States v. Miller*, 425 U.S. 435, 440–41 (1976) (holding that the Fourth Amendment does not prevent banks from turning over customer financial records even in the absence of a warrant or customer consent).

19. Anecdotal evidence suggests that private-sector support for counterterrorism operations has at times proven quite valuable. See OFFICE OF THE INSPECTOR GEN., DEP’T OF DEF. ET AL., UNCLASSIFIED REPORT ON THE PRESIDENT’S SURVEILLANCE PROGRAM 36 (2009) (noting that the Terrorist Surveillance Program “may have contributed to a counterterrorism success”); Brian Harmon et al., *Jet Passengers Foil Shoe-Bomb Suspect: “We Tied Him Up with Everything We Had,”* N.Y. DAILY NEWS, Dec. 23, 2001, at 3 (reporting that airline passengers and flight attendants overpowered a man with explosives packed in his shoe); Meyer, *supra* note 5 (describing a retail service technician’s assistance in foiling a domestic terrorism plot); Matthew Purdy & Lowell Bergman, *Unclear Danger: Inside the Lackawanna Terror Case*, N.Y. TIMES, Oct. 12, 2003, at A1 (noting the significance of an anonymous tip from an Arab-American citizen in identifying the Lackawanna Six); Shane & Lipton, *supra* note 8 (describing how airline passengers extinguished a fire and restrained the so-called Shoe Bomber when he tried to ignite a bomb on a commercial flight and how passengers did the same when Farouk Abdulmutallab attempted to ignite a bomb on a Christmas Day 2009 flight to Detroit); Jim VandeHei & Dan Eggen, *Cheney Cites Justifications for Domestic Eavesdropping*, WASH. POST, Jan. 5, 2006, at A2 (reporting on former Vice President Cheney’s claim that warrantless eavesdropping on U.S. persons helped thwart terrorist attacks). *But see* Lowell Bergman et al., *Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends*, N.Y. TIMES,

identities, institutions, and laws—in equally profound ways. This Symposium is devoted to big and pressing questions that arise at the intersection of national security, privacy, and technology. This contribution focuses on the proliferating deputization arrangements that operate at that intersection.

In what follows, I first describe the deputization phenomenon and survey a sampling of its manifestations, sophisticated and low-tech alike. Here, attention is devoted primarily to deputization arrangements of a corporate or employment nature to the exclusion of those programs targeting the general public.

Second, I identify and address the legal uncertainties and ambiguities underlying some of these deputization programs. The ambiguities arise as private actors—*turned*—deputies move out of the purely private realm, occupy unregulated or underregulated, hybridized private–public space, and participate in the exercise of sovereign power often far beyond what society currently contemplates and what the law currently constrains. These ambiguities in the deputies’ legal status at times enable the formation, operation, and success of many deputy partnerships, particularly those where private assistance is about something more than just force multiplication. Yet, they are just as relevant in creating or exacerbating the challenges these partnerships pose—challenges of social and economic dislocation, legal evasion, and even compromised security policy.

Third, by way of conclusion, I place homeland security deputization in some context. I begin this Part by considering possible contemporary analogues to deputization in the areas of criminal justice and economic regulation. I then sketch an analytical and normative framework—applicable in the homeland security context and, perhaps, beyond—for assessing whether, as an institutional matter, individual deputization arrangements operating in legally uncertain space ought to be deemed acceptable or rendered subject to greater regulatory constraints.²⁰

I. Surveying Deputies

Private involvement in matters of homeland security is hardly novel. Corporate and citizen cooperation in informing the government of supposedly anti-American activities at home and abroad dates far back in our

Jan. 17, 2006, at A1 (citing intelligence officials’ admissions that “virtually all” of the information that the National Security Agency collected in the aftermath of 9/11 led to dead ends).

20. It bears mentioning that this contribution builds on two of my recent projects—one that examines how private–public intelligence operations inhibit meaningful congressional and judicial oversight, see Michaels, *supra* note 9, and another that considers how privatization can and does expand the Executive’s ability to carry out policy objectives otherwise beyond its reach, see Jon D. Michaels, *Privatization’s Pretensions*, 77 U. CHI. L. REV. 717 (2010). This contribution provides a platform for synthesizing some of the material covered in that other work, and it builds on that platform to make novel interventions into the study of the use and misuse of legal-status distinctions between government actors and private actors in structuring private–public partnerships.

history.²¹ It is beyond the scope of this Article to recount this history with any depth or precision. For purposes of this inquiry, it suffices to note that by the mid-1970s, many of these private–public partnerships, especially the ones lacking a statutory or regulatory underpinning, had fallen into disfavor. In no small part, it was the post-Watergate hearings and investigations and the subsequent legislative enactments by a muscular majority in Congress hostile to executive prerogatives and secrets that served to rein in the Intelligence Community as well as its private collaborators.²²

When the demand for intelligence and intelligence operatives spiked after 9/11, the wide-scale solicitation of private assistance suddenly re-emerged as a respectable and perhaps even necessary practice. Some of the 9/11 hijackers had been living and training on U.S. soil for extended periods

21. See JAMES BAMFORD, *BODY OF SECRETS* 22 (2001) (recounting Western Union's assistance during World War II and the Cold War in providing the U.S. government with copies of foreign diplomatic dispatches); RON SUSKIND, *THE ONE PERCENT DOCTRINE* 35 (2006) (describing private intelligence and security assistance that dates back to the Civil War); TIM SHORRICK, *SPIES FOR HIRE* 76 (2008) (noting the corporate assistance to the NSA and CIA during the Cold War); Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1080–81 (2006) (describing Operation SHAMROCK, an NSA–telecom collaboration that facilitated U.S.-intelligence operations during the Cold War). While routinized, the relationships between the private sector and the government remained largely informal collaborations that lacked, for instance, a statutory or regulatory foundation. See INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS: HEARINGS BEFORE THE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, 94th Cong. 57–58 (1975) (statement of Sen. Frank Church, Chairman, Select Comm. to Study Governmental Operations with Respect to Intelligence Agencies) (noting corporate–government collaborations that were intentionally kept informal); Donohue, *supra* (“To keep [Operation SHAMROCK] under the radar, NSA deliberately refrained from formalizing the relationship in any sort of (traceable) document.”).

22. See Kathryn S. Olmsted, *CHALLENGING THE SECRET GOVERNMENT: THE POST-WATERGATE INVESTIGATIONS OF THE CIA AND FBI* 175–76 (1996) (describing legislative efforts to curb Executive discretion in domestic and foreign intelligence domains); Harold Hongju Koh, *Why the President (Almost) Always Wins in Foreign Affairs: Lessons of the Iran-Contra Affair*, 97 YALE L.J. 1255, 1270–71 (1988) (noting post-Watergate legislative initiatives seeking to narrow presidential discretion in matters of foreign affairs and intelligence gathering); see also William H. Jones, *AT&T Hits Wider Role in Wiretaps: Ma Bell Shuns Wider Wiretap Role*, WASH. POST, June 27, 1978, at E1 (indicating that after Watergate telecoms insisted on more formal legal processes instead of continuing to cooperate informally with intelligence agencies); Scott Shane, *Attention in NSA Debate Turns to Telecom Industry*, N.Y. TIMES, Feb. 11, 2006, at A11 (noting that in the wake of the 1970s' legislative inquiries and reforms the telecommunications industry insisted on arm's-length dealings with the intelligence agencies). See generally INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS: HEARINGS BEFORE THE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, *supra* note 21.

Notwithstanding the apparent hostility to private–public intelligence and security collaborations, some programs, ranging from workaday neighborhood watch associations to cutting-edge telecom partnerships, were created or expanded in the post-Watergate, pre-9/11 years. See, e.g., Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010 and in scattered sections of 18 U.S.C.) (imposing requirements on telecommunications carriers to assist in law enforcement efforts); OFFICE OF INSPECTOR GEN., *supra* note 4, at 2 (noting among other things that the Department of Transportation developed Highway Watch in 1998); Infragard: Public Private Partnership, <http://www.infragard.net/faq.php> (describing the joint FBI–private sector collaboration that in 1996 led to the founding of Infragard).

of time, interacting on a daily basis with flight instructors, neighbors, landlords, merchants, co-religionists, and classmates from language-training schools.²³ They also had been using banks, telecommunications providers, and airlines to facilitate their conspiracy.²⁴ Because of the inescapability of many of these points of contact²⁵ and the useful information that potentially could have been gleaned from these varied contacts (had civilians been primed to think of themselves as deputies), the Intelligence Community perceived the benefits of reaching out to citizens, employees, and corporations alike for assistance in identifying suspicious activity and preventing the next attack.²⁶

And, as the efforts of passengers who forced the crashing of United Flight 93 (rather than allow the hijackers to use the jet as a weapon) attested to,²⁷ it became clear that impromptu physical interventions might also be necessary, at least as a last line of defense in thwarting imminent attacks.²⁸

23. See 9/11 COMMISSION REPORT, *supra* note 9, at 215–53 (describing the social, commercial, financial, and employment-related interactions between the 9/11 hijackers and the American public); see also Wes Allison, *The Terrorists Next Door*, ST. PETERSBURG TIMES, Oct. 2, 2001, available at http://www.sptimes.com/News/100201/Floridian/The_terrorists_next_d.shtml (reporting on the lives of those 9/11 hijackers who lived in South Florida in the lead up to 9/11); Pam Belluck, *A Mundane Itinerary on the Eve of Terror*, N.Y. TIMES, Oct. 5, 2001, at A1 (recounting the activities of two 9/11 hijackers who had spent the day before the attacks in suburban Maine); John Cloud, *Atta's Odyssey*, TIME, Sept. 30, 2001 (describing Mohamed Atta's routine interactions with Americans); Rich Connell & Robert J. Lopez, *Portrait Emerges of an Islamic Hard-Liner*, L.A. TIMES, Dec. 12, 2001, at A18 (recounting Zacarias Moussaoui's life in Oklahoma).

24. See Prosecution's Ex. OG00020.2: Chronology of Events for Hijackers, United States v. Moussaoui, No. 01-455-A (E.D. Va.) <http://www.vaed.uscourts.gov/notablecases/moussaoui/exhibits/prosecution/OG00020-02.pdf> (detailing the hijackers' pre-9/11 use of ATMs for cash withdrawals, use of the Internet to access online travel records, and use of commercial airline services to travel around the United States); THOMAS R. ELDRIDGE ET AL., NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 AND TERRORIST TRAVEL: STAFF REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (2004), http://govinfo.library.unt.edu/911/staff_statements/911_TerrTrav_Monograph.pdf (detailing the hijackers' activities and interactions in the United States prior to the attacks).

25. See, e.g., William K. Rashbaum, *Police Tactic Against Terror: Let's Network*, N.Y. TIMES, Aug. 14, 2004, at B1 (quoting the New York City Deputy Commissioner for Intelligence as saying that “[t]he next Mohamed Atta is far more likely to intersect with someone from the private sector than a law enforcement officer”).

26. See, e.g., SOLOVE, *supra* note 11, at 166 (describing how intelligence officials can compile extensive personal profiles on suspects by examining the data generated by those suspects when they use the services of banks, telecoms, and airlines); James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1459 (2004) (noting the “depth and breadth of personally identifiable information available from private [commercial] sources, and the capacity to analyze such data and draw from it patterns, inferences, and knowledge”); Michaels, *supra* note 9, at 908–09 (describing the pivotal role the private sector can play in assisting government surveillance and intelligence-gathering efforts).

27. See Lane et al., *supra* note 8 (discussing the passenger-led revolt against hijackers on United 93).

28. See Brooks, *supra* note 8 (remarking on the initiative taken by passengers on commercial airlines in attempting to thwart terrorist attacks); see also Blake Morrison, *Airlines Push Passengers To Police Cabins*, USA TODAY, Oct. 17, 2001, at 1A (quoting one pilot as instructing the

The government thus likewise recognized the value of a mobilized citizenry cognizant of their responsibilities on public transit, around critical infrastructure, and elsewhere in times of crisis.²⁹

As it turns out, there was a convergence of interests. After 9/11, many corporate managers, rank-and-file workers, and average citizens were eager to do “their part”—and being encouraged to assist with safeguarding the nation from terrorism was more than adequate prompting.³⁰

This Part of the Article provides a brief overview of some of this outreach to the private sector. It focuses on actors who have been invited or solicited in their capacities as corporate executives or employees to provide counterterrorism assistance to the government.³¹ I call them “deputies” insofar as they are exercising some sovereign assistance, authority, or discretion far beyond what private individuals and organizations ordinarily are permitted or expected to do. Because I prioritize (1) the voluntary nature of deputy participation and (2) the uncertain legal terrain which they (and the government) must navigate in furthering these voluntary arrangements, I do not include within the ambit of discussion those operating pursuant to government contracts to assist in homeland security programs, or those compelled to support investigations through legal instruments such as court orders, subpoenas, or regulatory directives. Furthermore, because of the limited scope of this Symposium contribution, I do not attend to those individuals solicited as part of mass, open-ended appeals to the general public—even though they too could be considered deputies.³²

passengers: “Throw your shoes at them. A couple of you get up and tackle him. Beat the snot out of him. I don’t care.”).

29. See President George W. Bush, Address to Joint Session of Congress (Sept. 20, 2001), in H.R. DOC. NO. 107-122 (2003) (honoring a victim of United Flight 93 who risked his life endeavoring to stop the 9/11 hijackers from using the airplane as a weapon); Joe Sharkey, *There’s a New Deputy in the Sky*, N.Y. TIMES, Mar. 25, 2003, at C8 (noting that post-9/11 passengers are “much more vigilant now than ever”).

30. See Karen Brandon & Dahleen Glanton, *Americans on Alert for Terror: Agencies Swamped by Calls Reporting Suspicious Activity*, CHI. TRIB., Nov. 25, 2001, at C7 (“President Bush has asked citizens to help avert further terrorist attacks by looking out for suspicious activity, and Americans have responded with vigor.”); Ariana Eunjung Cha, *Watchdogs Seek Out the Web’s Bad Side*, WASH. POST, Apr. 25, 2005, at A1 (profiling a leading Internet vigilante who gravitated to online surveillance of Jihadist Web sites and chat rooms after being unable, for health reasons, to enlist in the military after 9/11); Ann Davis et al., *The Tattlers: A Nation of Tipsters Answers FBI’s Call in War on Terrorism—It’s Neighbor vs. Neighbor, as Agents are Swamped by 435,000 Citizen Leads*, WALL ST. J., Nov. 21, 2001, at A1 (describing an influx of calls to the authorities by members of the public reporting on what they perceive to be suspicious activities in their neighborhoods); Sam Howe Verhovek, *Air Passengers Vow To Resist Any Hijackers*, N.Y. TIMES, Oct. 11, 2001, at A1 (describing post-9/11 airline passengers’ apparent willingness to counter efforts by hijackers to take control of the plane); Ripley, *supra* note 4, at 39 (noting the enthusiasm among truckers for Highway Watch and characterizing it as a “morale booster for drivers”).

31. Several of the examples discussed in section B of this Part were examined in greater detail in Michaels, *supra* note 9, at 910–16.

32. To be sure, it would not be a stretch to call those individuals “deputies.” But the entreaties to the public are of a character quite different from the more direct and targeted appeals made by the government to specific industries, firms, and employee cohorts. Moreover, those members of the

Most of the deputy involvement is nonconfrontational. By and large, the government asks deputies to report on suspicious events viewed either in plain sight or in the course of having privileged access to private space, privileged access given to the deputies in their commercial capacities; or, the government requests access to the deputies' stores of data. But some involvement is more interventionist, including opening suspicious packages and independently analyzing data patterns for evidence of terrorist activity. Immediately below, I divide the deputy relationships into two groupings: programs targeting employees in the field (e.g., truck drivers, repair technicians, doormen) and programs geared toward corporate involvement at the management or institutional level. This division is not perfect, and there can be overlap between the two. Nevertheless, the division tracks four general, albeit not categorical, distinctions. First, whereas employees in the field are, by and large, deputized to be entrepreneurial in the assistance they provide—making their own determinations about what they view as unusual, dangerous, or suspicious—corporate management is typically responding to specific government queries and thus are providing more passive support. Second, employees in the field customarily offer eyewitness information about a specific person, incident, or transaction. The narratives they provide might be quite descriptive, but are just snapshots capturing a short period of time. By contrast, corporations tend to give the government aggregated information, numerous data points (about travel, purchases, or communications) on individuals and even large groups of individuals, often over extended periods of time. Third, employee-targeted programs are more difficult to keep secret than are corporate, data-driven programs. Many people are necessarily looped in for operations calling for thousands, or tens of thousands, of truck drivers, doormen, or service technicians to act as the government's eyes and ears. By contrast, data-driven initiatives can be administered far more discreetly, as they require the consent and cooperation of a comparatively small cohort of executives and IT specialists. Fourth, because the corporate-oriented partnerships tend to involve responding to specific queries, it may be easier for the government to monitor, assess, and control those relationships than it is for the authorities to do the same vis-à-vis employees in the field tasked with more open-ended surveillance responsibilities. As will be apparent in later parts of the Article, these differences are of significance, too, in gauging the types of challenges deputization engenders or exacerbates. For example, of the four challenges that will be highlighted in Part II, all four appear to be implicated by corporate-institutional deputization, but only two are likely to apply with any regularity to employee-oriented operations.

general public who heed the government's call typically occupy the force-multiplying space. For reasons explained below, this Article is particularly interested in deputies who serve the complementary purpose of providing the government with strategic advantages distinct from mere manpower support.

A. *Employee-Oriented Programs*

Because of their job responsibilities or the nature of their interactions with the public, segments of the American workforce have been identified as key homeland security resources. Included in this category of opportunistically situated workers are retail clerks, technicians who provide installation and repair services (cable TV, telephone, Internet, electricity, etc.), doormen, truckers, and longshoremen. By reaching out directly to workers or by entering into arrangements with their employers, unions, or industry trade associations,³³ the government has effectively deputized them to assist in security monitoring and enforcement.

Any discussion of labor-focused surveillance programs must begin with Operation TIPS. First referenced in President Bush's 2002 State of the Union Address,³⁴ TIPS was developed by the Justice Department as a "nationwide program giving millions of American truckers, letter carriers, train conductors, ship captains, utility employees, and others a formal way to report suspicious terrorist activity."³⁵ The government believed these workers were "well-positioned to recognize unusual events" and "report suspicious activity."³⁶ Especially significant were maintenance and delivery workers with direct access to individuals' homes (and thus well-positioned to observe that which is normally shielded from public scrutiny).³⁷ All of the

33. See, e.g., BART ELIAS, CONG. RESEARCH SERV., SECURING GENERAL AVIATION 21 (2009), available at <http://www.fas.org/sgp/crs/homesec/RL33194.pdf> (discussing the Airport Watch program); Sara Kehaulani Goo, *Private Pilots Enlisted for Security*, WASH. POST, Oct. 10, 2002, at A14 (describing Airport Watch and Operation TIPS); Swanson, *supra* note 2 (reporting on Highway Watch).

34. See President George W. Bush, *State of the Union Address*, WASH. POST, Jan. 30, 2002, at A16 (announcing the establishment of USA Freedom Corps, which included Operation TIPS); see also STANLEY, *supra* note 1, at 3–4 (distinguishing the surveillance-oriented TIPS program from the other Freedom Corps initiatives promoting citizen preparation and training in the event of civil emergencies).

35. Documents relating to Operation TIPS have long been removed from Justice Department Web sites, but have been preserved elsewhere. See, e.g., The Memory Hole: Website for Operation TIPS Quietly Changes, <http://www.thememoryhole.org/policestate/tips-changes.htm> (reproducing the text of the official Operation TIPS Web site, dated July 16, 2002).

36. *Id.*

37. See Editorial, *Ashcroft v. Americans*, BOS. GLOBE, July 17, 2002, at A22 (stating that Operation TIPS targets "letter carriers, meter readers, cable technicians, and other workers with access to private homes as informants to report to the Justice Department any activities they think suspicious"); STANLEY, *supra* note 1, at 3 ("Many of those targeted for inclusion in the scheme were workers with access to Americans' homes—utility workers, letter carriers and cable technicians—who were to report to the government anything that they considered an 'unusual or suspicious activity.'"). Compare *Katz v. United States*, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."), with *United States v. Kyllo*, 533 U.S. 27, 37 (2001) ("There is certainly no exception to the warrant requirement for the officer who barely cracks open the front door In the home . . . all details are intimate details, because the entire area is held safe from prying government eyes."); *Silverman v. United States*, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

participants were to be given access to special toll-free reporting numbers and their calls would be directly routed to the proper government agency.³⁸

Privacy concerns first forced the Justice Department to scale back Operation TIPS,³⁹ and, soon after, prompted Congress to defund the program.⁴⁰ TIPS's essence was nevertheless preserved through an array of more modest programs at the federal, state, and local levels.⁴¹ Some of those programs predated TIPS, taking on heightened significance in the wake of TIPS's cancellation. Others were fashioned anew.

First, maritime programs, one of the cornerstones of Operation TIPS, were detached and refashioned as more regional or local, stand-alone initiatives.⁴² For instance, Maine established Coastal Beacon, and recruited workers in the fishing and shipping industries to be vigilant and report on suspicious activities in the water and on the docks.⁴³ And, in the Midwest, Ohio created Eyes on the Water,⁴⁴ and Michigan developed River Watch.⁴⁵

A second program is Highway Watch.⁴⁶ Highway Watch enlisted the help of over three million truck drivers, creating "a potential army of eyes

38. The Memory Hole, *supra* note 35.

39. *See, e.g.*, MARTIN ALAN GREENBERG, *CITIZENS DEFENDING AMERICA: FROM COLONIAL TIMES TO THE AGE OF TERRORISM* 72–74 (2005) (quoting Senator Orrin Hatch as stating with respect to Operation TIPS that “[w]e don’t want to see a 1984 Orwellian-type situation here”); STANLEY, *supra* note 1, at 3 (noting that “the TIPS proposal was . . . met by a storm of outrage” that led the government to narrow its scope).

40. Homeland Security Act of 2002, Pub. L. No. 107-296, § 880, 116 Stat. 2135, 2245 (codified at 6 U.S.C. § 460 (2006)); *cf.* Department of Defense Appropriations Act, 2004, Pub. L. No. 108-87, § 8131, 117 Stat. 1054, 1102 (2003) (defunding the Terrorism Information Awareness data-mining project).

41. *See* Donohue, *supra* note 21, at 1133 (noting that “a plethora of programs” emerged in the wake of Operation TIPS’s demise). For instance, Florida reproduced key features of the disbanded TIPS program within its boundaries. *See, e.g.*, Brian Baskin, *Workers Recruited in War on Terror*, *ORLANDO SENTINEL*, July 8, 2004, at A1 (noting that Florida’s programs are similar to the disbanded federal program); STANLEY, *supra* note 1, at 5 (noting that key aspects of Operation TIPS have been replicated at the state level by Florida).

42. *See* STANLEY, *supra* note 1, at 5 n.10. Stanley notes that whereas Operation TIPS would have created a centralized maritime program, subsequent efforts by the Coast Guard have aimed for far more decentralized operations. *Id.*

43. *Id.* at 4. Acknowledging the program’s lineage, President Bush called Coastal Beacon “one of the most innovative TIP[S] programs in the country.” Press Release, White House, President Promotes Citizen Corps for Safer Communities (Apr. 8, 2002), <http://georgewbush-whitehouse.archives.gov/news/releases/2002/04/20020408-4.html>.

44. STANLEY, *supra* note 1, at 5.

45. *Id.*; Michigan State Police: Homeland Security River Watch Program, http://www.michigan.gov/msp/0,1607,7-123-1589_3492-73050--,00.html.

46. GREENBERG, *supra* note 39, at 224–25; OFFICE OF INSPECTOR GEN., *supra* note 4, at 1–2. Highway Watch, a private–public partnership, actually predates what is commonly called the Global War on Terror. In 1998, the Trucking Association started the program, with funding from the Department of Transportation, to report generally on transportation emergencies, such as hazardous road conditions and vehicle crashes. After 9/11, its scope was expanded in recognition of the threats of terrorist attacks on U.S. soil, and its governmental responsibilities were transferred to the new Department of Homeland Security. *See* OFFICE OF INSPECTOR GEN., *supra* note 4, at 2 (noting the post-9/11 expansion and re-orientation of Highway Watch).

and ears to monitor for security threats.”⁴⁷ At its height, more than 800,000 truckers were considered “active” members patrolling the nation’s highways.⁴⁸

A third initiative taps into the general aviation network of airplane pilots and airport workers.⁴⁹ It was these workers who had contact with, and some suspicious interactions with, the al Qaeda hijackers prior to the attacks of 9/11.⁵⁰ Dubbed Airport Watch, the joint Transportation Security Administration–Aircraft Owners and Pilots Association program provides specialized training in detecting and reporting on suspicious activities.⁵¹

A fourth set of partnerships brings doormen and building maintenance workers into the counterterrorism fold.⁵² To date, tens of thousands of doormen, superintendents, and other building workers have received training and instruction regarding the detection and reporting of suspicious activities.⁵³ Supported by the building-owners industry as well as the unions representing building workers,⁵⁴ the workers-turned-deputies have been called “natural allies” of the police.⁵⁵ They are expected to alert the police to any suspicious packages or vehicles; and, they are encouraged to file reports on tenants with little or no furniture as well as on would-be renters seeking to pay in cash or via newly opened bank accounts.⁵⁶

47. STANLEY, *supra* note 1, at 5.

48. OFFICE OF INSPECTOR GEN., *supra* note 4, at 4. The program has been temporarily suspended while DHS shifts resources away from the Trucking Association and to a government contractor that will help administer the program. Samuel Lowenberg, *Truckers Lose DHS Contract*, POLITICO, May 16, 2008, <http://www.politico.com/news/stories/0508/10412.html>.

49. ELIAS, *supra* note 33, at 35; Alonso-Zaldivar, *supra* note 3; Goo, *supra* note 33.

50. See 9/11 COMMISSION REPORT, *supra* note 9, at 221–27 (describing suspicious behavior exhibited by some of the 9/11 hijackers during their flight-training programs); see also Transcript of Record at 747–62, *United States v. Moussaoui*, No. 1:01cr455 (E.D. Va. Mar. 9, 2006), available at <http://cryptome.org/usa-v-zm-030906-01.htm> (statement of Moussaoui’s flight school instructor) (recounting suspicious behavior of Zacarias Moussaoui in flight school); ELIAS, *supra* note 33, at 1, 12–17 (noting that the 9/11 hijackers were trained on general aviation planes and made suspicious inquiries regarding the purchase of small aircraft).

51. See ELIAS, *supra* note 33, at 22 (noting that Airport Watch involves the “cooperation and participation of pilots, airport tenants, and airport workers to observe and report suspicious activity”); see also AOPA’s Airport Watch, <http://aopa.org/airportwatch/> (describing the general aviation community’s partnership with the Transportation Security Administration that involves more than 600,000 private pilots and airport workers acting as the government’s “eyes and ears for observing and reporting suspicious activity”).

52. See Goldman, *supra* note 8 (describing surveillance training and reporting responsibilities for doormen and other residential-building workers); Swanson, *supra* note 2 (noting the incorporation of doormen and other residential-building workers into the homeland security fold).

53. Goldman, *supra* note 8.

54. *Id.*

55. *Id.* (quoting New York City Police Commissioner Raymond Kelly).

56. See *id.* (reporting that “doormen are advised to be on the lookout for cars and trucks that seem out of place or are parked too long near buildings” and “[s]uperintendents are told to be vigilant in monitoring people with little or no furniture or newly opened bank accounts who move into apartments.”). As the 9/11 Commission reported, some of the 9/11 terrorists revealed telltale signs of being suspicious tenants, including attempting to pay deposits for apartment rentals with

B. Management-Oriented Programs

The government has not only reached out to employee groups. It has also forged ties with business executives and managers to acquire data, surveillance footage, tips on suspicious customers, and physical evidence. From what we know, some relationships are driven by a convergence of patriotic interests.⁵⁷ Others have been secured through a carrots-and-sticks approach. Reportedly, the promise of government contracts,⁵⁸ the offer to share privileged, advanced information,⁵⁹ and the placement of corporate executives on high-profile private-public task forces⁶⁰ have at times been held forth as rewards for private cooperation.⁶¹

Among the collaborations that have trickled into the public domain is the Terrorist Surveillance Program (TSP).⁶² Under the TSP, the NSA “secretly arranged with top officials of major telecommunications companies to gain access to large telecommunications switches carrying the bulk of

cash and owning little furniture. See 9/11 COMMISSION REPORT, *supra* note 9, at 219 (reporting that a real-estate agent rejected an attempt by two of the hijackers to pay cash for a deposit on an apartment rental and noting that two hijackers moved into an apartment with no furniture and no possessions). Whether those practices provide significantly sensitive guidance in exposing terrorists is, of course, a debatable proposition; but having workers focus on such tenant practices speaks to the enthusiasm and, perhaps, hubris of being able to discern terrorist patterns from atypical behavioral cues.

57. See, e.g., SUSKIND, *supra* note 21, at 209–11 (describing how then-CIA Director George Tenet appealed to the patriotism of Western Union executives to secure their cooperation).

58. In particular, there have been allegations that the government has canceled or withheld contracts in retaliation against firms that refused to cooperate in intelligence operations. See Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at A1 (“In one meeting, an NSA representative suggested that . . . Qwest’s footdragging might affect its ability to get future classified work with the government. Like other big telecommunications companies, Qwest already had classified contracts and hoped to get more.”); Ellen Nakashima & Dan Eggen, *Former CEO Says U.S. Punished Phone Firm*, WASH. POST, Oct. 13, 2007, at A1 (citing a Qwest executive’s claim that the NSA canceled contracts worth hundreds of millions of dollars as punishment for the telecom refusing to participate in the call-data program).

59. For examples of firms receiving strategically important information in exchange for their participation, see Infragard: Public-Private Partnership, *supra* note 22; Matthew Rothschild, *The FBI Deputizes Business*, PROGRESSIVE, Mar. 20, 2008, available at https://www.progressive.org/mag_rothschild0308.html; and, Block, *supra* note 7. Rothschild notes that upon learning of a possible terrorist threat to some bridges in California, federal officials informed Enron and Morgan Stanley—both members of the corporate-FBI strategic partnership (called Infragard)—well before notifying state officials, including the Governor. Rothschild, *supra*, at 21–22.

60. See Block, *supra* note 7 (noting that FedEx has been named to the FBI’s regional terrorism task force).

61. At other times, it appears that companies are selling access to information in ways that make them appear more like profiteers than partners, let alone coerced accomplices. See Kim Zetter, *Yahoo Issues Takedown Notice for Spying Price List*, WIRED, Dec. 4, 2009, <http://www.wired.com/threatlevel/2009/12/yahoo-spy-prices> (reporting on the comprehensive pricing scheme that Yahoo has established for facilitating law enforcement search requests).

62. See OFFICE OF INSPECTOR GEN., *supra* note 4, at 1; see generally James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1 (describing the TSP).

America's telephone calls."⁶³ The access, granted "without warrants or court orders,"⁶⁴ enabled government eavesdroppers to monitor the content of millions of international telephone calls and electronic correspondence, including those where one of the parties was on U.S. soil.⁶⁵ Because access to this information typically would have required the government to secure court authorization pursuant to the terms of the Foreign Intelligence Surveillance Act of 1978 (FISA),⁶⁶ the deputization arrangement has been described as "open[ing] up America's domestic telecommunications network to the NSA in unprecedented and deeply troubling new ways, and represent[ing] a radical shift in the accepted policies and practices of the modern U.S. intelligence community."⁶⁷

Second, the so-called "NSA call-data program" involved major telecommunications companies agreeing to provide the NSA with stores of telephonic and electronic metadata, including metadata generated from domestic calls and e-mails.⁶⁸ Metadata includes telephone numbers, IP addresses, and e-mail accounts of correspondents and the times that communications took place.⁶⁹ The NSA then crunches that information through sophisticated data-mining programs with the aim of piecing together relationships and patterns of relationships in a way that reveals terrorist activity and terrorists themselves.⁷⁰

63. JAMES RISEN, *STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION* 48 (2006).

64. Cauley & Diamond, *supra* note 1. One federal district court declared the program illegal. *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006). That decision was reversed by a divided panel for want of standing. *ACLU v. NSA*, 493 F.3d 644 (6th Cir. 2007), *cert. denied*, 552 U.S. 1179 (2008); *see also* *Al-Haramain Islamic Found. v. Obama*, MDL Docket No. 06-1791, 2010 WL 1244349 (N.D. Cal. Mar. 31, 2010) (rejecting the government's state-secrets barrier to reviewing the TSP and entering summary judgment in favor of the plaintiffs in light of the Government's failure to oppose plaintiffs' merits arguments).

65. RISEN, *supra* note 63, at 48; Cauley & Diamond, *supra* note 1.

66. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered titles of U.S.C.). In the aftermath of the TSP, FISA has been amended several times. *See* Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (to be codified at 50 U.S.C. §§ 1803, 1805a-1805c); FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2468 (to be codified in scattered sections of 50 U.S.C.).

67. RISEN, *supra* note 63, at 44.

68. Cauley, *supra* note 58; Saul Hansell & Eric Lichtblau, *U.S. Wants Internet Companies To Keep Web-Surfing Records*, N.Y. TIMES, June 2, 2006, at A15. It is worth noting that Qwest's former CEO reported first being approached by the government in early 2001, months before the attacks of September 11. Scott Shane, *Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11*, N.Y. TIMES, Oct. 14, 2007, at A27.

69. *See* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611 (2003).

70. *See* Michaels, *supra* note 9, at 912; Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 261 (2008); K.A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 1, 33-35 (2003). Though the bulk of legal and academic attention is typically focused on the content of communications (and thus on eavesdropping), *see*, for example, Orin S. Kerr, *A User's Guide to the Stored Communications Act*,

Third, another recently disclosed telecom program began as a contractual arrangement to facilitate the processing of FBI subpoenas (specifically, National Security Letters,⁷¹ or NSLs).⁷² Evidently, it soon morphed into something far more open-ended, accommodating, and, perhaps, legally dubious.⁷³ With representatives of the major telecommunications firms detailed to FBI offices, assigned FBI e-mail accounts, granted access to FBI computer networks, and invited to socialize after work with the government agents,⁷⁴ the telecoms soon dispensed with asking to be served with NSLs as a condition of processing the data queries.⁷⁵ Indeed, the telecoms reportedly informed FBI officials that the government could bypass the requirements for producing a valid NSL and instead invoke its so-called “exigent-letter” authority⁷⁶ to acquire the sought-after information more quickly (and with a lower evidentiary showing).⁷⁷ The telecoms even generated the exigent-letter authority forms for the FBI to sign.⁷⁸ It appears as if even this shortcut was eventually circumvented, as the telecoms subsequently agreed to give the FBI “sneak peeks” at data to see if the underlying information would be worth the agents’ time to initiate formal requests (via exigent letters or NSLs).⁷⁹ More interesting, at least for present purposes, than this gradual erosion of legal protocols was the proactive engagement of the telecom employees. The telecom workers not only

and a Legislator’s Guide to Amending It, 72 GEO. WASH. L. REV. 1208, 1229 n. 142 (2004), scholars have also recognized the exceptional utility of compiling virtual dossiers and piecing together virtual itineraries of suspects’ communications over months or even years. See, e.g., Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1287–88 (2004).

71. See, e.g., 18 U.S.C. § 2709(a) (2006), since limited by *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 862 (2d Cir. 2008). For a more detailed discussion of NSLs, see OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF NATIONAL SECURITY LETTERS, at x–xiv (2007), <http://www.usdoj.gov/oig/special/s0703b/final.pdf> [hereinafter FBI USE OF NATIONAL SECURITY LETTERS].

72. OFFICE OF INSPECTOR GEN., U.S. DEP’T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 12 (2010), <http://www.justice.gov/oig/special/s1001r.pdf> [hereinafter FBI USE OF EXIGENT LETTERS]. For an earlier instance of reported improprieties involving the FBI’s use of NSLs, see FBI USE OF NATIONAL SECURITY LETTERS, *supra* note 71.

73. See John Solomon & Carrie Johnson, *FBI Broke Law for Years in Phone Record Searches*, WASH. POST, Jan. 20, 2010, at A1.

74. FBI USE OF EXIGENT LETTERS, *supra* note 72, at 25; Ryan Singel, *FBI, Telecoms Teamed To Breach Wiretap Laws*, WIRED, Jan. 21, 2010, <http://www.wired.com/threatlevel/2010/01/fbi-att-verizon-violated-wiretapping-laws/#ixzz0e3YLimPT>.

75. FBI USE OF EXIGENT LETTERS, *supra* note 72, at 33.

76. See 18 U.S.C. § 2702(c)(4) (2006) (authorizing emergency exceptions to the usual NSL requirements in cases where the government has a good-faith belief that a delay in acquiring the information could result in serious injury or the loss of life).

77. See FBI USE OF EXIGENT LETTERS, *supra* note 72, at 31–32 (noting that the FBI agent in charge of the program first learned of exigent-letter authority from “Company A” and that based on the information provided by “Company A” the agents began invoking exigent-letter authority).

78. *Id.* at 33.

79. *Id.* at 47–50.

proposed and facilitated the shortcuts (which presumably were outside of the terms of the government contracts⁸⁰) but also took the initiative regarding what they saw as “very interesting” patterns of use among phone numbers and “strongly suggest[ed]” that the FBI investigate certain leads further.⁸¹ Tellingly, at least one of the telecom employees created an e-mail folder entitled “TEAM USA” and sent out e-mails to FBI agents that “began with a greeting to ‘Team.’”⁸²

Fourth, soon after 9/11 the CIA approached Western Union executives and told them “this country is in a fight for its survival. What [we’re] asking is that you and your company be patriots.”⁸³ Ever since, Western Union has reportedly been alerting the government to suspicious wire transfers, turning over data detailing transactions by persons of interest to the government, and sending intelligence officials real-time video images of those wiring money from Western Union storefronts.⁸⁴

Fifth, FedEx, which prior to 9/11 steadfastly denied law enforcement requests for assistance,⁸⁵ has since committed itself fully to U.S. counterterrorism efforts.⁸⁶ Its ready cooperation, which includes opening and inspecting packages at the government’s behest,⁸⁷ stands in contrast to that of its main competitors, United Parcel Service and the United States Postal Service—both of which refuse to service government requests absent legal compulsion.⁸⁸

Sixth, through Operation Nexus, the New York City Police Department has established collaborative relationships with businesses that may be of particular interest to terrorists.⁸⁹ Defining “interest” broadly, police have reached out to more than 30,000 businesses—including scuba shops, plastic

80. And, which were presumably not in the financial interests of the firms, in no small part because such informal facilitation may have exposed the telecoms to legal liabilities. Many of the actual terms of the contracts are censored in the Inspector General’s published report. Based on the nonredacted portions of the report, the contracts do not appear to call for the fluid exchange of information that appears to have taken place. *See id.* at 20–24.

81. *Id.* at 47–49.

82. *Id.* at 25.

83. SUSKIND, *supra* note 21, at 211. Western Union has a long history of providing such support for the government. *See supra* note 21 and accompanying text.

84. SUSKIND, *supra* note 21, at 208–11; Michaels, *supra* note 9, at 914.

85. Block, *supra* note 7.

86. *See id.* (quoting FedEx’s CEO as committing his company to cooperate with the government “up to and including the line on which we would be doing a disservice to our shareholders”).

87. *Id.*

88. *See* Corky Siemaszko, *FedEx Delivers—Info to the Feds*, N.Y. DAILY NEWS, June 5, 2005, at 24 (citing both UPS and the USPS as unwilling to provide customer information to the government without a warrant); *see also* Dan Eggen, *Bush Warned About Mail-Opening Authority*, WASH. POST, Jan. 5, 2007, at A3; Isaac Baker, *Little Support for TIPS*, NEWSDAY, July 21, 2002, at A25.

89. *See* NYPD Shield: Operation Nexus, <http://www.nypdshield.org/public/nexus.nypd> (detailing a program designed to foster counterterrorism collaboration between the police department and the private sector).

surgeons, hardware stores, and self-storage facilities, located within and outside of the five boroughs.⁹⁰ One of the program's goals is to encourage businesses to be sensitive to suspicious inquiries and transactions and to file reports with the authorities.⁹¹

II. Underregulation and Uncertainty in the Deputized Space

The descriptive accounts offered above identify cartographic information about how two landscapes—that of homeland security and that of civil and corporate society—intersect and overlap through deputization programs and practices. They also provide us with the tools to do more: first, to locate the legal uncertainties that underlie the transformation of private actors into deputies who participate in the exercise of sovereign authority (often without fully bearing the legal responsibility commensurate with that exercise); second, to understand the challenges—e.g., disruptions to civil society, the market economy, the rule of law, and even the counterterrorism operations themselves—engendered or exacerbated by the legal uncertainties clouding the deputized space; and, third, to begin the process of developing a framework for differentiating acceptable from intolerable manifestations of deputization that take place in unregulated or underregulated space. This Part of the Article takes up the first two tasks. Sketching an evaluative framework will be reserved for Part III.

A. *Deputization's Legal-Status Uncertainties*

Status is critical to the deputization agenda, especially where deputization is something more than simply an exercise in force multiplication. Deputy relationships that provide something more—e.g., special access or the bypassing of legal restrictions imposed exclusively on government actors—pivot in no small part on the diffusion, distortion, and re-invention of traditional status designations of the private actors-turned-deputies. To develop these arrangements, deputization's architects frequently build in unregulated or underregulated space, gaps in the legal landscape where statutory, regulatory, and decisional law have not fully defined the scope of government or private-sector conduct. The architects then deploy the deputies and direct them to perform (or to support) a range of state-security duties in this space. In turn, the deputies find themselves in a form of identitarian limbo: no longer confined to the boundaries of their civilian and corporate existence, but far from being full-fledged government agents; no longer driven exclusively by market pressures, but far from being inattentive to profits or their employment responsibilities.

90. See William Finnegan, *The Terrorism Beat: How is the N.Y.P.D. Defending the City?*, NEW YORKER, July 25, 2005, at 58; Judith Miller, *On the Front Line in the War on Terrorism*, CITY J., Summer 2007, available at http://www.city-journal.org/html/17_3_preventing_terrorism.html; Rashbaum, *supra* note 25.

91. See Miller, *supra* note 90.

The deputies' limbo—and the legal ambiguities and uncertainties surrounding their status and the status of the hybrid, private–public space they occupy—is empowering, frustrating, and dangerous, sometimes all at once. Because of their ostensible private status (and the stickiness of that status notwithstanding the realities of deputies crossing over into public, sovereign domains), these civilians-*turned*-deputies at times are able to further government aims with less notice, resistance, or legal consequence than if they were actually to join the governmental ranks or otherwise shed their private personas. This is precisely why deputization is not simply about force multiplication: There are special benefits that accompany the marshaling and martialization of the private sector (*qua* private sector), and one of the chief benefits is the government's ability to leverage this status ambiguity in favor of deeper reaching (and not just more numerous) homeland security programs.

This legal uncertainty or ambiguity also opens the door to coercive, discriminatory, or destructive practices within largely unregulated private–public space. Among them, there are newfound opportunities for the government to pressure deputies, as well as opportunities for deputies to go beyond what the government wants or expects them to do *vis-à-vis* exercising sovereign discretion, either in furtherance of the deputies' business aims or in furtherance of the deputies' own conception of the public good. Moreover, the uncertainty may deter conscientious would-be deputies and simultaneously attract the more risk-seeking civilians; it thus suggests the likelihood of selection and recruitment problems that may undermine deputization's homeland security goals.

B. The Challenges of Ambiguity

In what follows, I discuss some of the challenges created or exacerbated by the ambiguous and uncertain status issues that surface in deputized space. These challenges span a wide range of policy and legal domains including national and homeland security, due process, separation of powers, and market competition.⁹² Specifically, I highlight four types of ambiguity and work through their effects *vis-à-vis* the deputization agenda: (1) government actors conflating how they interact and negotiate with would-be deputies and how they generally interact and negotiate with private firms and industries, what I call the Market Distortion Challenge; (2) deputies conflating their own public and private roles, what I call the Misappropriation Challenge; (3) deputies' uncertain assessment of uncertain legal space, what I call the Risk Selection Challenge; and, (4) the legal regime's uncertainty in distinguishing deputies from nondeputized civilians, what I call the *De Facto*

92. Because there is no shortage of discussions regarding privacy, either in this Symposium or in the scholarly literature in general, I do not focus on the privacy encroachments even though they are broadly implicated and likely exacerbated by the legal uncertainty undergirding most of the deputization arrangements under examination.

State Action Challenge. Hardly constituting an exhaustive list, these four issues are just a sampling of some of the procedural and substantive challenges that deputization invites.⁹³

1. *The Market Distortion Challenge: Government Actors Conflating Treatment of Deputies and Private Firms.*—As alluded to above, the government solicits deputy participation through a number of channels. It might apply moral suasion, appealing to patriotism and volunteerism to induce private firms to enter into deputy relationships.⁹⁴ Or, it might resort to doling out perks or threatening punitive action.⁹⁵

Outside of the voluntary deputization context, the government can compel participation by invoking statutory and regulatory authority to require⁹⁶ or encourage disclosures;⁹⁷ government officials can also enter into contracts and thus purchase support services from the private sector or

93. A few notes before proceeding. First, although identitarian limbo and the uncertain legal status of deputies lie at the heart of the concerns to be discussed in this section, it does not follow that the converse—a deputization regime grounded in legal certainty—is a necessary or sufficient antidote. This issue will be addressed in greater detail in Part III. Second, although I recognize that what I term a “challenge” incident to deputization is subject to some normative contestation, the scope of this Symposium contribution limits the depth with which I can thoroughly defend the challenges as normatively charged phenomena. Third, deputization, even as narrowly addressed in this inquiry, operates along a spectrum between some regulatory foundation and no regulatory foundation. Some programs are, at the very least, publicly announced and funded, with congressional appropriations going to conduct outreach and training and to pay for the dedicated hotlines and other support measures that facilitate deputization. See, e.g., *supra* notes 46–48 and accompanying text (discussing Highway Watch); *supra* notes 49–51 and accompanying text (discussing Airport Watch). These programs may be audited regularly (as a practical reality, if not a statutory imperative) and not only in response to a front-page scandal. See, e.g., OFFICE OF INSPECTOR GEN., *supra* note 4. Others are largely (and intentionally) under the radar, and within that category we have some programs—such as the TSP—that seem to violate existing laws, and also programs that simply avail themselves of the opportunity to operate in unregulated space. See, e.g., *supra* subpart I(B); cf. Adrian Vermeule, *Our Schmittian Administrative Law*, 122 HARV. L. REV. 1095, 1103–31 (2009) (describing “black” and “grey” holes in the administrative state). Thus, my analysis sometimes encompasses all deputization programs, and sometimes just a particular subset. Fourth, the distinctions drawn in Part I between employee and corporate-oriented deputization programs are relevant here, too. By and large, many of the corporate-oriented arrangements are likely to implicate all four sets of challenges described in this section. Employee programs, on the other hand, are more likely to implicate only the latter two.

94. See *supra* note 57 and accompanying text.

95. See *supra* notes 58–60 and accompanying text.

96. For a canvassing of some such legal authorities to compel assistance, see Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 289–305 (2008).

97. See, e.g., Critical Infrastructure Information Act (CIIA) of 2002, 6 U.S.C. §§ 131–134 (2006). The CIIA includes a blueprint for private–public cooperation and for private–public quid pro quos. Among other things, the Act immunizes corporations from civil liability for weaknesses in their infrastructure, provided those weaknesses are first disclosed to the government. *Id.* § 133(a)(1). The government encourages and rewards such disclosures as a way of increasing the likelihood of its knowing what corporate vulnerabilities exist and how they might endanger national, economic, or homeland security.

simply buy privately held information.⁹⁸ Through these legal and contractual channels, the government has (1) some flexibility in terms of how best to structure partnership relationships; (2) express authority to encroach on the autonomy of the market economy;⁹⁹ and, (3) greater legal clarity as to what roles the private participants will play. But what is different about deputization in contrast to legal compulsion or contract—even though the difference may be more a matter of degree than kind—is that where deputization lacks regulatory authority, guidance, and transparency, it opens the hybrid private–public space to an inordinate amount of ad hoc horse trading. This horse trading not only influences private-sector participation in counterterrorism efforts. It may also spill out of the homeland security deputization space altogether and more generally distort markets and market decisions.

Consider the carrots and sticks reportedly used to entice cooperation and punish refusals to participate. Less efficient firms willing to play ball in matters of homeland security could gain a comparative advantage in the marketplace over more efficient firms hesitant to cooperate. Indeed, if the market is otherwise competitive and the perks of participation are significant, the latter group of companies will face a difficult decision: forgo government contracts and access to strategic information—at some risk to profits and market share—or go against their business obligations (e.g., contractual assurances of consumer privacy protections) or legal misgivings in order to stay viable.¹⁰⁰

98. For discussions of data brokering, see Michaels, *supra* note 9, at 917–19; and Joshua L. Simmons, Note, *Buying You: The Government's Use of Fourth-Parties to Launder Data About "the People,"* 2009 COLUM. BUS. L. REV. 950.

99. See, e.g., Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010 and in scattered sections of 18 U.S.C.) (requiring telecommunications providers to ensure that their technologies are compatible with those the government uses to engage in lawful surveillance and monitoring efforts); Davis–Bacon Act, ch. 411, 46 Stat. 1494 (1931) (requiring government contractors to pay prevailing wages for public-works projects).

100. Perhaps a firm such as UPS might experience such pressure. As noted above, FedEx, UPS's chief rival, has received a range of national security perks, which might be viewed as compensation for the courier company's steadfast and public support of government intelligence operations. See *supra* Michaels, *supra* note 9, at 914–16; notes 60, 85–88 and accompanying text. Among other things, FedEx was the first private company to be named to a seat on the FBI's regional terrorism task force. It was also awarded an exceptional license to establish its own police force with investigatory and arrest powers. See *supra* Michaels, *supra* note 9, at 914–15, Block, *supra* note 7. As a dutiful deputy, FedEx receives information early. See Gary Fields, *FedEx Takes Direct Approach to Terrorism*, WALL ST. J., Oct. 9, 2003, at A4 (noting that members of the regional task forces are given “more-sensitive and specific data regarding terrorist threats than businesses usually receive”). Might UPS, which reportedly rejected at least some of the government's requests for counterterrorism assistance, be left out in the cold? If so, it likely incurs greater risk by not having the same access FedEx does to counterterrorism intelligence. For instance, if UPS facilities aren't as carefully safeguarded (or if UPS has to expend more of its own resources on *private* security initiatives because it isn't receiving courtesy tips from the government), might that be a reason for customers and shareholders to switch to FedEx? See *id.* (“[T]he FedEx representative [receiving the more sensitive and specific information] can signal the company to take preventative actions. If the task force learns certain kinds of explosives are being

The distortions might not end there. Shareholders—the firms’ *principals*—might become uneasy about managers—the firms’ *agents*—entering into these voluntary relationships, or uneasy about managers forgetting about the market incentives altogether when approached by the government and told to put country ahead of corporation.¹⁰¹ These principals might then seek to lessen the delegated discretion accorded to their agents.¹⁰² But keeping management on a tighter leash in response to the fear that the executives will otherwise commit too fully to deputization could lead to an inefficient allocation of principal–agent discretion and responsibility in terms of general strategic planning or day-to-day operations, thus introducing additional distortions into the market economy.

Whether deputization’s horse trading strikes a better or worse balance on the security–liberty continuum than if the government used its existing statutory authorities (or sought new power) to compel and contract for assistance is, for present purposes, beside the point. What instead matters is twofold. First, on the substance, we may be discomfited by the government tipping the scales of market competition based on which firms cozy up with the intelligence agencies. In essence, the government is using deputies’ dual status against them by striking at their private, nondeputy interests. The government does so not only in a way that can warp market competition, but also in a way that is contrary to how it tends to approach the private sector in, for example, the ordinary government–contracting context, perhaps a close alternative to deputization arrangements. When soliciting and then evaluating bids for government contracts, agencies are ordinarily required to ensure nondiscriminatory treatment among competitors such that “winners” and “losers” are designated as such on the basis of price and quality¹⁰³—not, say,

used by terrorists in Asia, for instance, the representative can alert the company to install specialized explosives detectors there.”)

101. See *supra* note 57 and accompanying text.

102. For seminal discussions of principal–agent concerns, see Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs, and Ownership Structure*, 3 J. FIN. ECON. 305, 312–30, 333–43 (1976); and Armen A. Alchian & Harold Demsetz, *Production, Information Costs, and Economic Organization*, 62 AM. ECON. REV. 777, 785–90 (1972).

103. See, e.g., Competition In Contracting Act (CICA) of 1984, Pub. L. No. 98-369, 98 Stat. 1175 (codified at 40 U.S.C. § 471 et seq.; 41 U.S.C. § 251 et seq.). Some exceptions to the general rule that winners are chosen based entirely on the strength of their bid proposals exist; by and large, however, those bases for discriminating among firms on non-market terms have been authorized by statute or regulation. See, e.g., Veterans Benefit Act of 2003, Pub. L. No. 108-183, 117 Stat. 2662 (codified at 15 U.S.C. § 657f (2003)) (authorizing preferences for contract bids from small businesses owned by service-disabled veterans). It is also true that, for better or worse, the government could—and sometimes might need to—tailor its contracting specifications such that certain firms are likely to be the only ones qualified to handle delegated responsibilities. See, e.g., Dan Baum, *Nation Builders for Hire*, N.Y. TIMES, June 22, 2003, § 6 (Magazine), at 32 (“KBR got the Iraqi oil-field contract without having to compete for it because, according to the Army’s classified contingency plan for repairing Iraq’s infrastructure, KBR was the only company with the skills, resources, and security clearances to do the job on short notice.”).

Moreover, it is of course the case that the government could impose legal conditions on firms selectively, serving some with onerous subpoenas and court orders, while simply asking other firms

on whether firms contributed to the President's campaign coffers or funneled information to the intelligence agencies. In addition, the government's commodification of vital security information is yet another way of complicating and confusing the dual roles of deputies and private businesses. Here too, by rationing information¹⁰⁴ and giving advanced notice only to cooperative firms,¹⁰⁵ which then are in a better position to safeguard their assets and customers (and save money by not having to independently analyze security threats), the government is affecting the private market.

Second, as a procedural matter, there is the question of democratic legitimacy in how the government interacts with would-be deputies. With the advent of deputization and the informality associated with many of its non-statutory, non-regulatory arrangements, there are now two scripts for engaging the private sector: the official script that contains a variety of authorized inducements and coercive directives¹⁰⁶ and the unofficial script that leaves the inducements and the coercive strategies to the imagination and discretion of the intelligence officials.¹⁰⁷ That is to say, however much the government already reaches into the day-to-day business of corporate America, and however much discretion it has in making those interventions,¹⁰⁸ it does so typically constrained by the scope of democratic authority, an insistence on transparency, procedural regularity, nondiscrimination, and the imperatives of reasoned public administration.¹⁰⁹ It can

to comply. Thus, my point is not that the government is otherwise—outside of deputization, that is—entirely evenhanded; rather, simply that deputization may exacerbate the potential for unequal treatment across firms.

104. Assuming the firms aren't themselves security risks, there is little justification for not sharing this nonscarce information with other American businesses (other than to hold it out as a reward or in-kind payment).

105. See *supra* notes 59, 100 and accompanying text.

106. *E.g.*, Critical Infrastructure Information Act (CIIA) of 2002, Pub. L. No. 107-296, §§ 211–215, 116 Stat. 2135, 2150 (2002) (codified at 6 U.S.C. §§ 131–134 (2002)).

107. *Cf.* HBO v. FCC, 567 F.2d 9, 53–54 (D.C. Cir. 1977) (criticizing *ex parte* contacts in the course of agency rulemaking and noting that “[e]ven the possibility that there is here one administrative record for the public and this court and another for the Commission and those ‘in the know’ is intolerable”).

108. See, *e.g.*, Heckler v. Chaney, 470 U.S. 821, 834–35 (1985) (declaring agency decisions as against whom to bring enforcement actions generally unreviewable); FTC v. Standard Oil Co. of Cal., 449 U.S. 232, 238–46 (1980) (finding FTC issuance of a complaint was not judicially reviewable before the conclusion of the administrative adjudication, notwithstanding the complaint's immediate disruptive effects on business).

109. See Heckler, 470 U.S. at 848 (Marshall, J., concurring). Justice Marshall states:

[T]he *sine qua non* of the APA [Administrative Procedure Act] was to alter inherited judicial reluctance to constrain the exercise of discretionary administrative power—to rationalize and make fairer the exercise of such discretion. Since passage of the APA, the sustained effort of administrative law has been to “continuously narrow the category of actions considered to be so discretionary as to be exempted from review.” Discretion may well be necessary to carry out a variety of important administrative functions, but discretion can be a veil for laziness, corruption, incompetency, lack of will, or other motives, and for that reason, “the presence of discretion should not bar a court from considering a claim of illegal or arbitrary use of discretion.” Judicial

hardly be assured that these commitments will carry over into the deputization context. Indeed, the concerns associated with ad hoc interactions with corporations are especially acute in the secretive world of intelligence, where external scrutiny and effective oversight are often wanting,¹¹⁰ and where firms are in a weaker position to cry foul (both because the classified nature of the proposed arrangements prevents them from speaking out and because the firms will be fearful that their speaking out in opposition to government entreaties will be viewed as unpatriotic). Thus, the shift from even a relatively flexible but law-based paradigm to one where deputization occurs in the gaps and shadows of regulation is that much more significant.

2. *The Misappropriation Challenge: Deputies Conflating Their Deputy and Private Roles.*—A different concern, but one that also stems from the fluidity and ambiguity of status roles, is the possibility that businesses agreeing to serve as deputies will misappropriate the intelligence information they are receiving from the government to deny services to customers who are targets of investigations. In many cases, the government needs to disclose some information to the corporations to facilitate the processing of surveillance queries; indeed, that's likely the sole purpose of the government's disclosure. For the firms to take the information and use it for business decisions is in one respect to be expected given the firms' dual identities as facilitators of counterterrorism operations and also as for-profit

review is available under the APA in the absence of a clear and convincing demonstration that Congress intended to preclude it precisely so that agencies, whether in rulemaking, adjudicating, acting or failing to act, do not become stagnant backwaters of caprice and lawlessness.

Id. (internal citations omitted). See *Ethyl Corp. v. EPA*, 541 F.2d 1, 68 (D.C. Cir. 1976) (Leventhal, J. concurring) ("Congress has been willing to delegate . . . broadly and courts have upheld such delegation because there is court review to assure that the agency exercises its delegated power within statutory limits, and that it fleshes out objectives within those limits by an administration that is not irrational or discriminatory."); see also *Massachusetts v. EPA*, 549 U.S. 497, 533–34 (2007) (requiring agency to provide reasoned justification for refusing to render a scientific judgment relevant to whether greenhouse gases should be regulated); *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 56–57 (1983) (invalidating agency rescission of rule where the agency fails to articulate a reasoned explanation for the rescission); *Citizens To Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402, 417–20 (1971) (rejecting agency decision where Secretary failed to make findings in support of agency decision); Jody Freeman & Adrian Vermeule, *Massachusetts v. EPA: From Politics to Expertise*, 2007 SUP. CT. REV. 51, 87–92, 97 (highlighting an expertise-forcing approach by courts reviewing agency decisions and non-decisions).

110. See James A. Baker, *Intelligence Oversight*, 45 HARV. J. ON LEGIS. 199, 205 (2008); Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2318–22 (2006) (emphasizing that foreign affairs and national security are domains where legislative and judicial scrutiny is often lacking); Memorandum from Alfred Cummings, Specialist in Intelligence and Nat'l Sec., Cong. Research Serv., to Senator Dianne Feinstein (Dec. 14, 2005), available at <http://feinstein.senate.gov/crs-intel.htm> (noting Congress's comparative inability, because of the limited information the Executive provides, to independently assess the quality of intelligence and the operations).

enterprises.¹¹¹ But it is also highly problematic as a matter of due process and also substantively, as the private appropriation of that information may undercut national security objectives.

For a variety of reasons, the government might give firms a list of named targets (or phone numbers, bank account numbers, or IP addresses) without distinguishing among sure-fire terrorists, likely terrorists, possible confederates, and friends, family, and colleagues not themselves suspected of involvement in terrorist conspiracies. The government might simply not be at liberty, or otherwise inclined, to share that information with the firms. Or it might not yet know enough to draw such distinctions.¹¹² Indeed, as has been reported, the government might know so little that it asks companies to do their own analysis to ascertain a target's "community of interest."¹¹³ The government's casting of a wide net might be particularly likely in deputization contexts if the reason for the request being channeled through a deputization partnership is that the government lacks the evidentiary basis to compel disclosure through court orders or administrative subpoenas.¹¹⁴

In some settings, firms are legally required to deny services to individuals named on government watch lists. The No-Fly list is of that

111. The decision to mix the government search request with the business bottom line is an almost unavoidable outcome when deputies are asked to occupy hybridized space and must, at the end of the day, prioritize their private (business) responsibilities over their public charges. See *Dodge v. Ford Motor Co.*, 170 N.W. 668, 684 (Mich. 1919) (emphasizing the primary duty of corporate managers to maximize shareholder profits); see also AUDIT DIV., U.S. DEP'T OF JUSTICE, AUDIT REPORT 08-03, SUMMARY OF FINDINGS: THE FEDERAL BUREAU OF INVESTIGATION'S MANAGEMENT OF CONFIDENTIAL CASE FUNDS AND TELECOMMUNICATION COSTS 4 (2008), available at <http://www.usdoj.gov/oig/reports/FBI/a0803/final.pdf> (describing a particularly cold-blooded business decision by a telecom working very closely with the FBI on counterterrorism operations that resulted in a temporary disabling of the government's access to electronic surveillance and lost evidence); cf. Daniel I. Gordon, *Organizational Conflicts of Interest: A Growing Integrity Challenge*, 35 PUB. CONT. L.J. 25 (2005). Of course, an argument could be made that prioritizing the government requests in the context of homeland security would be in the long-term financial interests of the corporations. Cf. *Shlensky v. Wrigley*, 237 N.E.2d 776, 777-78 (Ill. App. 2d 1968); *A.P. Smith Mfg. Co. v. Barlow*, 98 A.2d 581, 583-86 (N.J. 1953).

112. See Eric Lichtblau, *F.B.I. Made 'Blanket' Demands for Phone Records*, N.Y. TIMES, Mar. 14, 2008, at A1.

113. See Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. TIMES, Sept. 9, 2007, at A1 ("The scope of the demands for information could be seen in an August 2005 letter seeking the call records for particular phone numbers under suspicion. The letter closed by saying: 'Additionally, please provide a community of interest for the telephone numbers in the attached list.'"); see also FBI USE OF EXIGENT LETTERS, *supra* note 72, at 47-49 (detailing corporate involvement in developing a list of names associated with a particular target).

114. See FREDERICK A.O. SCHWARZ, JR. & AZIZ Z. HUO, UNCHECKED AND UNBALANCED: PRESIDENTIAL POWER IN A TIME OF TERROR 132 (2007) (describing efforts by the intelligence agencies to proceed informally on the basis of "thinner evidence"); Carol D. Leonning & Dafna Lanzer, *Judges on Surveillance Court To Be Briefed on Spy Program*, WASH. POST, Dec. 22, 2005, at A1 (noting the Bush Administration's contentions that the statutory and regulatory evidentiary hurdles were often too great for the intelligence agencies to secure the desired authorization they needed to conduct electronic surveillance).

vein,¹¹⁵ as are lists generated by Treasury's Office of Foreign Assets Control.¹¹⁶ But in other contexts, and absent the regulatory directives that give effect to those official lists (that is to say, the government generates the suspect list internally and then orders private companies to refuse access or service to would-be customers named to the list), when the government provides names to private firms to facilitate data-mining or surveillance operations, it isn't intending for the companies to use that information as they see fit in their business dealings. Yet, as some suspect, firms might be using those lists to deny services to customers included on the government query sheets.¹¹⁷

Decisions by the companies to deny services might be efforts to mete out private justice: the bank, telecom, or travel company takes matters into its own hands, doing its part to punish the perceived evildoers. Thus, it cancels lines of credit, disconnects Internet service, or makes it more difficult for the named individuals to arrange transportation or secure employment. Or, the misappropriation and denial of services are acts of self-interest: firms might not want to, among other things, extend credit to someone about to be deported or detained. More to the point, what company wants to be known for furnishing a group of terrorists with the rental car used to set off a bomb, or to have hosted on its servers the Jihadist chat room out of which emerged a lethal band of terrorists.¹¹⁸

Yet in denying often-essential services,¹¹⁹ the companies are working off scant information and making decisions without any solid grounding in due process¹²⁰ or factual substantiation.¹²¹ For all the firms know, the

115. See 49 U.S.C. § 114(h) (Supp. I 2001) (providing authority for the imposition of No-Fly lists on commercial airlines); see also Jeffrey Kahn, *International Travel and the Constitution*, 56 UCLA L. REV. 271, 321–23 (2008); Justin Florence, Note, *Making the No Fly List Fly*, 115 YALE L.J. 2148, 2155–59 (2006). See generally Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1274 (2008) (noting the No-Fly list's high incidence of false positives).

116. Exec. Order 13,224, 66 Fed. Reg. 49,079 (Sept. 23, 2001); see also *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Pub. L. No. 107-56, § 314, 115 Stat. 272, 307–08 (codified at 31 U.S.C. § 5311 (2006)).

117. See Sara B. Miller, *Blacklisted by the Bank*, CHRISTIAN SCI. MONITOR, Aug. 25, 2003, <http://www.csmonitor.com/2003/0825/p15s01-wmcn.html>; Kim Zetter, *Big Business Becoming Big Brother*, WIRED, Aug. 9, 2004, http://wired.com/news/conflict/0,2100,64492,00.html?tw=wn_tophead_1 (describing the possibility that firms are cross-checking government surveillance lists to deny services and offers of employment to individuals named to those lists).

118. Indeed, firms might find themselves in a Catch-22: assuming a company does not appropriate the information, subsequent revelations that government security agencies gave the company the names of the individuals who later perpetrated an attack will lead to questions why the firm continued to do business with those individuals.

119. These decisions will no doubt disproportionately affect certain, already vulnerable communities.

120. Historically, common carriers under the common law and regulated industries under the Interstate Commerce Act have been sanctioned for engaging in discriminatory practices or arbitrary denials of service. See Joseph Kearney & Thomas Merrill, *The Great Transformation of Regulated Industries*, 98 COLUM. L. REV. 1323, 1325, 1331–32 (1998) (noting that the 1887 Interstate

“target” is simply a person who has communicated with the real suspect or just happens to have the same name as someone suspected of being involved in terrorism. In those cases, there is no moral or strategic basis for denying service. Or, the government is monitoring a bunch of guppies in an effort to lure and reel in the big fish—and cutting off services to those guppies might tip off a terrorist cell and force it to go deeper underground.¹²² In that situation, there might well be plausible reasons for the firms to terminate service as a matter of justice and financial and reputational self-interest. But there obviously are also national security reasons why the government might want these “guppy” customers to continue going about their business. Accordingly, the misappropriation is not just an issue of insufficient due process and discriminatory business practices, but also an issue of undermining security objectives.

3. *The Risk Selection Challenge: Deputies' Uncertain Assessment of Uncertain Space.*—Uncertainty surfaces, too, with respect to how deputies view themselves, their status, and their responsibilities in hybridized space. Some may be drawn to the apparent freedom afforded to step outside of the confines of civilian life; they can aid in counterterrorism operations without truly having to give themselves over to a public calling (by formally entering government service)—and perhaps without incurring the same legal liabilities for acting overzealously that government officials would face. For others, stepping outside of civilian life may be unnerving. Without clearly defined duties and without clear legal guidance regarding their responsibilities in this private–public space, they might not be willing to take the chance that they will in fact be beyond sanction.

The ambiguity regarding the hybridized space invites something somewhat akin to an adverse selection problem,¹²³ and thus threatens to

Commerce Act imposed a nondiscrimination obligation on firms in industries covered by the Act); Joseph William Singer, *No Right To Exclude: Public Accommodations and Private Property*, 90 NW. U. L. REV. 1283, 1439 (1996) (describing common law obligations imposed on common carriers).

In addition to there likely being little meaningful process prior to the businesses' decisions to, say, terminate services, the issue of private appropriation of government information—and the effect of that appropriation—also touches upon long-contested questions about what remedies individuals have when the government furthers, but does not carry out or compel, a private injury or deprivation of rights. *Cf.*, e.g., *Paul v. Davis*, 424 U.S. 693 (1976).

121. *See Miller*, *supra* note 117 (noting businesses' continued reliance on outdated government lists of suspected terrorists that the government itself has since updated, revised, or withdrawn).

122. This concern has been voiced with respect to Internet vigilantes, concerned citizens typically working on their own (i.e., without government support or knowledge) to disable Jihadist Web sites and chat rooms. The Internet vigilantes' efforts have drawn the ire of government officials, who lose access to valuable information when the vigilantes take matters into their own hands and shut down sites that are, oftentimes, already carefully being monitored by the intelligence agencies. For a more extensive discussion, see *infra* notes 124–25.

123. *Cf.* George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 493–94 (1970).

undermine security policy. Specifically, responsible actors (ordinarily, the very ones we want heeding the deputization call) will be risk adverse in light of this uncertainty and commit only modestly and tentatively. Risk-seeking, perhaps even reckless, actors will, on the other hand, be far less deterred by the potential liabilities incident to deputization; and this group might come to occupy a disproportionately large and active segment of the deputy pool. In the case, say, of doormen or repairmen, the careful, cautious employees may forswear or shirk deputy responsibilities precisely because their snooping around might subject them to legal liability or even physical retaliation. Those with more bravado and fewer reservations would push forward, not only willing to search and investigate, but also willing to search and investigate in a relatively aggressive fashion.¹²⁴ As a substantive matter, this

124. Perhaps an extreme version of the risk-seeking deputy is the vigilante. We have seen private individuals and groups decide, on their own initiative, to insert themselves into the world of deputization and into this hybridized space. Among them are the civilian border patrols that have begun organizing, monitoring and, at times, capturing and detaining those trying to enter the country illegally. These groups, which include the Minutemen, are often motivated largely by anti-immigrant sentiments having mostly to do with economics and culture, by worries that terrorists are sneaking into the country through porous borders, and by their belief that the U.S. Border Patrol is ill-equipped or ill-disposed to stop them. Accordingly, various militia groups have staged public demonstrations and set up armed outposts in Arizona and California, as well as along the nation's northern border with Canada. See David A. Fahrenthold, *On Patrol in Vt., Minutemen Are the Outsiders*, WASH. POST, Oct. 31, 2005, at A2 (reporting on the New England branch of the Minutemen); Anna Gorman, *Volunteers To Patrol Border Near San Diego*, L.A. TIMES, May 5, 2005, at B1 [hereinafter Gorman, *Volunteers*] (attributing the upswing in volunteer border patrol membership in part to the members' perception that the Bush Administration was failing to secure the nation's borders); Michael Leahy, *Crossing the Line*, WASH. POST, Mar. 19, 2006, (Magazine), at 14 (chronicling efforts by private anti-immigration groups to mount border patrols and monitor labor sites suspected of employing undocumented aliens). Such groups have been criticized and labeled "vigilantes" by the likes of then-President George W. Bush for their excessive use of violence and their interference with the official Border Patrol operations. Leslie Berestein, *Legal Groups to Watch County "Minutemen,"* S.D. UNION-TRIB., July 1, 2005, at B4; Anna Gorman, *Patrol Delays Launch*, L.A. TIMES, June 9, 2005, at B6. But, Governor Schwarzenegger of California and even Bush's own chief immigration enforcement official have expressed greater enthusiasm for their efforts. See Gorman, *Volunteers*, *supra* (noting Governor Schwarzenegger's support for the Minutemen group, which he said had "done a terrific job" in contrast to the federal government that was "not doing [its] job"); Solomon Moore, *Immigration Official Praises Citizen Patrols*, L.A. TIMES, July 21, 2005, at B6 (reporting on then-Customs and Border Protection Commissioner Robert Bonner's praise of citizen patrols on the U.S.-Mexico border).

A second group is the so-called Internet vigilantes, who were briefly mentioned above. See *supra* notes 15, 122. Some Internet watchdogs go no further than alerting the government to the existence (and substantive content) of extremist Web sites. See, e.g., Erika Hayasaki, *Tracking Terrorists from Her Home Computer*, L.A. TIMES, Jan. 11, 2009, at A17; Nadya Labi, *Jihad 2.0*, ATLANTIC MONTHLY, July-Aug. 2006, at 102; Benjamin Wallace-Wells, *Private Jihad*, NEW YORKER, May 29, 2006, at 28. Others take it a step or two further. Among this cohort is Internet Haganah, an organization with a moniker that harkens back to the Jewish paramilitary group operating under the British mandate in Palestine prior to Israeli independence. Haganah takes a more activist approach, committing itself to monitoring and *disabling* Jihadist Web sites. Typically, Haganah is able to disable a Web site by overloading the servers or by pressuring the Web sites' Internet service providers to take down the site. Howard Altman, *Web Warriors Track Down, Close Jihadist Internet Sites*, TAMPA TRIB., Nov. 17, 2005, at 12; Michael Snider, *On Osama's Trail*, MACLEAN'S, Nov. 15, 2004, at 94.

phenomenon seems to make deputization less attractive to at least some government officials. The “responsible” would-be participants retreat, and the most aggressive participants dominate the landscape—potentially sapping resources as government officials must keep a close watch on them to make sure they do not harass suspects or otherwise frustrate ongoing investigations by dispensing their own forms of justice (on their own timetables).¹²⁵

4. *De Facto State-Action Challenge: The Legal Regime’s Uncertainty in Distinguishing Deputies from Nondeputized Civilians.*—As stated above, there is more to deputization than its force-multiplying effects. Of seemingly greater practical and normative purchase than deputization’s force multiplication is deputization’s leveraging of the private sector to gain faster, deeper, or less legally encumbered access to people, places, and data. That is to say, faster, deeper, or less legally encumbered than what the government could do were it limited to using its own personnel.

The private sector’s comparative advantage is an artifact of a predeputized landscape.¹²⁶ In some important respects, private actors’ conduct is not subject to as strict regulatory, statutory, or constitutional limitations. In part this is because private actors are not assumed to be exercising

125. As one terrorism expert, expressing concerns with the counterproductive role being played by Internet vigilantes, notes:

From a law enforcement perspective, it is better to keep those sites online. If you really want to shut them down, don’t go after some pimply faced Web master, who is a low-level member. Do what you do in a mafia case. Pull in the small guy to reel in bigger fish.

Altman, *supra* note 124, at 12; *see also* Cha, *supra* note 30 (quoting a federal official who called Haganah “a grave threat to national security”); Snider, *supra* note 124, at 94 (characterizing the work of Haganah and others as “hacktivism” and counterproductive); Carmen Gentile, *Cyber Vigilantes Track Extremist Web Sites, Intelligence Experts Balk at Effort*, FOXNEWS.COM, Mar. 22, 2008, <http://www.foxnews.com/story/0,2933,340613,00.html> (citing experts’ frustration with Internet vigilantes for interfering with government investigations); Brad Stone, *Heroes or Nettlesome Hacks?*, NEWSWEEK.COM, July 2005, <http://www.newsweek.com/id/50330> (noting the Intelligence Community’s annoyance over vigilantes’ efforts that “scuttle ongoing surveillance . . . and eventually force terrorists to find less observable ways of spreading their message”).

Likewise, concerns have been raised regarding the counterproductive and abusive role played by private border patrols. *See, e.g.*, Randal C. Archibold, *A Border Watcher Finds Himself Under Scrutiny*, N.Y. TIMES, Nov. 24, 2006, at A1 (reporting on allegations that a self-appointed border patrolman in Arizona falsely imprisoned, threatened, and physically abused undocumented aliens as well as lawful U.S. residents who he assumed entered the country illegally); Tim Gaynor, *Border Vigilantism Alleged in Ariz. Case: Rancher Accused of Holding Mexican American Family at Gunpoint*, WASH. POST, Nov. 15, 2006, at A3 (highlighting the increase in “vigilante violence” along the U.S.–Mexico border); Jesse McKinley & Malia Wollan, *New Border Fear: Violence by a Rogue Militia*, N.Y. TIMES, June 27, 2009, at A9 (discussing border violence believed to be perpetrated by members of the Minutemen militia); *see also* Nick Madigan, *Police Investigate Killings of Illegal Immigrants in Arizona Desert*, N.Y. TIMES, Oct. 23, 2002, at A15 (discussing the accusation that a militia group funds its border-patrol activities by robbing drug dealers).

126. It is probably more accurate to say the artifact of a preprivatized landscape. *See, e.g.*, Michaels, *supra* note 20.

or facilitating state power.¹²⁷ By contrast, the ordinarily more stringent rules placed on government actors may be justified precisely in terms of the apprehensions associated with their capacity to exercise state sovereignty. Amazon.com can do a lot with the information it gathers. It can botch your order, improperly customize your “favorites” settings, sell information about your preferences to marketers or other retailers, and even reveal your credit card information. But—unlike the State—it is not capable of using that information to order criminal investigations, terminate government benefits, or designate you as a suspicious person. Given the relative innocuousness of private power (not to mention the commercial benefits to firms and customers alike that come with businesses trafficking in consumers’ personal information), there are legitimate reasons not to overly limit the ability of private actors to collect, analyze, and even sell personal information.¹²⁸

Deputization thus comes as a wolf in sheep’s clothing and creates problems for the durability of this private–public distinction.¹²⁹ But, for now, so long as deputization has taken root and these legal distinctions perdure, opportunities for exploitation abound. Using private proxies increases the government’s legal scope of counterterrorism activities.¹³⁰ For example, FedEx may in its ostensibly private capacity open customers’ packages. A

127. See, e.g., *NCAA v. Tarkanian*, 488 U.S. 179, 191 (1988) (“Embedded in our Fourteenth Amendment jurisprudence is a dichotomy between state action, which is subject to strict scrutiny . . . and private conduct, against which the Amendment affords no shield, no matter how unfair that conduct may be.”).

128. See James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 13 (2003) (noting that businesses that collect information are “looking for better and more efficient ways” to operate); Anita Ramasastry, *Data Mining, National Security and the “Adverse Inference” Problem*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 757, 758 (2006) (stating that the collection of personal data by businesses helps “to maximize profit and to improve consumer experience”); see also Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 415 (2002) (noting the public’s willingness to disclose personal information to businesses to facilitate commercial endeavors); Declan McCullagh, *It’s Been 10 Years: Why Won’t People Pay for Privacy?*, CNET NEWS, Jan. 28, 2010, http://news.cnet.com/8301-13578_3-10443575-38.html (describing studies indicating that people readily disclose personal information, including passwords, in exchange for nominal commercial benefits).

129. Needless to say, deputization is hardly the only phenomenon that creates problems for the durability of private–public distinction. For example, some instances of government contracting do as well. See, e.g., Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285, 1289–90 (2003); Minow, *supra* note 10, at 994–95.

130. Deputization is not novel here. Far from it. Landmark cases have long allowed third-party transfers of information to the government in the absence of the target’s express consent. *Smith v. Maryland*, 442 U.S. 735, 743–45 (1979); *United States v. Miller*, 425 U.S. 435, 440–41 (1976); see also *United States v. Matlock*, 415 U.S. 164, 171 (1974) (“[C]onsent of one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared.”); *Coolidge v. New Hampshire*, 403 U.S. 443, 484–90 (1971) (holding that a wife could search and seize her husband’s property and voluntarily turn it over to the police absent a warrant). What is important with respect to the homeland security deputies is the greater potential for institutionalizing these relationships—that is, not just the occasional call by the authorities to the bank for third-party records or the sporadic request made to spouses or other household residents by police and prosecutors to obtain information absent warrants or express consent, but instead the systematic harnessing of private resources in service of long-term relationships.

FedEx–government operation might not trigger the same constitutional warrant requirements that attach where government officials directly seek such access. This is because state action is not consistently ascribed to private parties, even those working with the government.¹³¹ To date, the applicability of the Fourth Amendment to nongovernmental personnel tends to be limited to situations where the private party is acting as an agent of, or in conjunction with, the police.¹³² Depending on how the FedEx–government arrangement is actually structured,¹³³ there may be opportunities to *encourage*—rather than *direct*—FedEx activism that leads the company to exercise ostensibly independent judgment in opening up suspicious packages. That is, unlike an unambiguous agent of the government, FedEx’s status as an occupier of amorphous public and private space—and as a business still looking out for its own commercial interests (when it, among other things, decides to seize packages)—may create enough of a break from the state-action nexus to permit it to act without the attendant constitutional liability.¹³⁴

131. See, e.g., *Correctional Servs. Corp. v. Malesko*, 534 U.S. 61, 63 (2001) (declining to recognize a *Bivens* claim against a private prison facility operating pursuant to a federal contract); *Rendell-Baker v. Kohn*, 457 U.S. 830, 843 (1982) (refusing to allow a § 1983 suit to lie against a private school funded almost entirely by government to educate “maladjusted” students). But see *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 936–37 (1982) (authorizing a § 1983 suit against a private firm acting jointly with the Commonwealth of Virginia in exercising “state action”).

132. See *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (“This Court has . . . consistently construed [Fourth Amendment] protection as proscribing only governmental action; it is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.” (internal citations omitted)); see also *United States v. Momoh*, 427 F.3d 137, 141 (1st Cir. 2005) (considering for purposes of determining constitutional liability the government’s role in instigating or directing the private search, the government’s control over the private actor’s search, and whether the private actor is primarily aiding the government or furthering its own objectives); *United States v. Robinson*, 390 F.3d 853, 872 (6th Cir. 2004) (“[T]o trigger Fourth Amendment protection under an agency theory, ‘the police must have instigated, encouraged, or participated in the search,’ and ‘the individual must have engaged in the search with the intent of assisting the police in their investigative efforts.’” (quoting *United States v. Lambert*, 771 F.2d 83, 89 (6th Cir. 1985))); *United States v. Smith*, 383 F.3d 700, 705 (8th Cir. 2004) (listing among the factors to be considered in determining whether a private citizen was acting as an agent of the government “whether the government had knowledge of and acquiesced in the intrusive conduct; whether the citizen intended to assist law enforcement agents or instead acted to further his own purposes; and whether the citizen acted at the government’s request”).

133. See Block, *supra* note 7; Fields, *supra* note 100; Siemaszko, *supra* note 88, at 24. As mentioned above, both UPS and the Postal Service have refused entreaties to provide law enforcement and intelligence agencies with similar assistance. See *supra* note 88 and accompanying text.

Coincidentally, *Jacobsen* involved FedEx employees opening a package, finding contraband, and reporting their discovery to law enforcement officials—all without triggering a Fourth Amendment violation. 466 U.S. at 111, 114–17.

134. See, e.g., *United States v. Hall*, 142 F.3d 988, 995 (7th Cir. 1988) (holding that an independent search by a computer repair firm that led the firm to contact authorities did not implicate the Fourth Amendment); see also Simmons, *supra* note 98, at 986–87 (describing informal private–public cooperation on searches that led to criminal prosecution). But see *United States v. Walther*, 652 F.2d 788, 793 (9th Cir. 1981) (finding state action in an airline-carrier search

Similarly, government partnerships with the private sector create a channel that enables the bypassing of otherwise applicable statutory restrictions on the gathering of personal information. For example, certain foundational federal privacy laws focus primarily on limiting what the government can acquire.¹³⁵ With the exception of a few named industries expressly included in the statutes' coverage, private actors are unencumbered by such laws and can acquire the information and freely pass it on to the government.¹³⁶ A private-public partnership thus gives the government access to more expansive searches than would be permissible were the government forced to rely exclusively on its own personnel.¹³⁷

In terms of physical surveillance, the deputization of workers might give the government greater warrantless entrée to private space. Cable repairmen are admitted where the police likely are refused, presumably on the reasonable understanding that the repairmen's purpose is to install HBO, not scope out the living room for Jihadist literature. This isn't a legal evasion per se, because a police officer invited to enter a home could just as readily scan the bookshelves in search of militant tracts.¹³⁸ But it is far more likely that a resident will freely admit a cable repairman into her home but not a police officer. The greater comfort with the technician is predicated in part on the desire to have a commercial service performed, and in part on perhaps now-naïve and outdated assumptions about status—about the ostensibly exclusive business nature of the technician's visit, and about the technician's ostensibly limited ability to generate law enforcement problems for the resident.¹³⁹

Deputization in these contexts changes the nature of consent. As suggested, surely the government could similarly bypass the extant legal limitations on opening packages, acquiring data, or entering homes by first obtaining permission from the package senders or recipients, from those whose data is sought, and from the residents whose homes it wants to search. But, with deputies, a different, easier brand of consent can be obtained. Consent is displaced onto third parties—the volunteer firms and employees—

where the government "had knowledge of a particular pattern of search activity . . . and had acquiesced in such activity").

135. See, e.g., Privacy Act of 1974, 5 U.S.C. § 552a (2006).

136. See Danielle Keats Citron, *The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 255 (2007). Citron notes that "the private sector's collection of sensitive personal information remains largely unregulated by federal law. While federal legislation governs the security of personal data stored by federal agencies, similar federal restrictions apply only to a narrow set of private entities, such as financial institutions, credit agencies, and health care providers." *Id.*; see Michaels, *supra* note 20, at 721–23; Michaels, *supra* note 9, at 908–09 & n.23 (2008); see also Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 365–67 (describing how statutory restrictions imposed on the government when collecting data covered under the Privacy Act of 1974 and the Fair Credit Reporting Act of 1970 can be bypassed if information is first privately gathered).

137. See Michaels, *supra* note 20, at 741–42.

138. The observation of what might be considered suspicious materials is likely to prompt, if anything, additional surveillance or investigatory work, rather than an actual, immediate seizure.

139. See *supra* note 18 and accompanying text.

who likewise must be convinced to accede to the government's request. The convincing is far easier, however, given that these third parties, unlike the suspects, do not personally bear the brunt of the costs of the invasion or encroachment.

Leveraging the private sector in this respect no doubt increases the number and severity of privacy encroachments.¹⁴⁰ But this practice has broader consequences as well. The first such consequence has to do with private-public relationships writ large and the law's uncertainty vis-à-vis occupants of this dualist space; that is, deputies straddling the private-public divide work in the interstices of legal rules that assume—perhaps too readily—a more complete divide between private and public action. Thus, the deputization relationships blur the boundary of state action. They complicate the roles and responsibilities not only of deputies but also other private actors assisting the government in various capacities.¹⁴¹ The second consequence has to do with the Executive Branch's ability to deploy private-sector resources in efforts to overcome restrictions placed by Congress and the courts on its (public) power.¹⁴² We typically think of outsourcing and reliance on the private sector as the government *ceding* sovereignty and abrogating its own authority.¹⁴³ In practice, however, elements of deputization are clearly power aggrandizing to Executive Branch officials and implicate important separation of powers concerns.¹⁴⁴

III. Situating Deputization

Having described deputization practices and examined some challenges brought about by these distinctively underregulated collaborations, this Part offers three concluding discussions.

A. Contemporary Analogues

First, deputization is not unique to homeland security. Besides its historical forerunners noted above,¹⁴⁵ there are contemporary analogues in more conventional areas of law enforcement as well as in other contexts entirely

140. See *supra* note 92.

141. An obvious set of private actors potentially affected by such line-blurring is government contractors. Contracting out for government services is so pervasive today that the annual expenditures for contractors at the federal, state, and local levels combined is now in excess of \$1 trillion. Jeffrey L. Dunoff, *Linking International Markets and Global Justice*, 107 MICH. L. REV. 1039, 1041, nn.5–6 (2009).

142. We see similar efforts outside of the intelligence-gathering context as well. See Michaels, *supra* note 10; see also Matthew Diller, *The Revolution in Welfare Administration: Rules, Discretion, and Entrepreneurial Government*, 75 N.Y.U. L. REV. 1121, 1182–83 (2000).

143. See VERKUIL, *supra* note 10, at 102–14; Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367, 1400–06 (2003).

144. Cf. Michaels, *supra* note 20 *passim* (addressing this claim in the context of government contractors).

145. See *supra* notes 21–22 and accompanying text.

divorced from criminal justice and national security. In the law enforcement setting, the largely opaque, unregulated police practice of employing informants to provide tips, assist in sting operations, and elicit confessions and other admissions is not altogether unlike the homeland security deputization protocols. Though their employment has long vexed legal analysts,¹⁴⁶ informants continue to occupy dualist space—certainly not police, but something more than (or different from) civic-minded citizens.¹⁴⁷ For their cooperation, informants may receive benefits in the form of monetary compensation,¹⁴⁸ more lenient sentencing for their own infractions, or outright immunity for past or ongoing criminality.¹⁴⁹ The analogy isn't perfect, however. The lack of clear standards for regulating the informants' role in matters of criminal justice might not be readily attributable to emergency conditions, which are often invoked as a justification for the ad hoc nature of some post-9/11 counterterrorism practices.¹⁵⁰ Nor might the explanation for the general failure to regulate informants in a systematic fashion—or for the related reluctance to make the informant agreements more transparent—be as easily grounded in the need for secrecy as is the case with homeland security deputization. Important as it likely is to conceal the identities of individual informants in active criminal investigations (at least for some stretch of time), there nevertheless seems to be comparatively little need to conceal informant programs' goals and protocols in the same way that counterterrorism agencies must protect their "sources and methods."¹⁵¹

A variant of deputization seems to have arisen in another contemporary context: in efforts to manage the global financial meltdown of 2008. Numerous reports have pointed to a series of meetings where top government officials sat down with the titans of Wall Street, and—at times, without clear

146. See, e.g., George C. Harris, *Testimony for Sale: The Law and Ethics of Snitches and Experts*, 28 PEPP. L. REV. 1, 57 (2000); Alexandra Natapoff, *Snitching: The Institutional and Communal Consequences*, 73 U. CIN. L. REV. 645 (2004); Daniel Richman, *Cooperating Defendants: The Costs and Benefits of Purchasing Information from Scoundrels*, 8 FED. SENT'G REP. 292 (1996); Ian Weinstein, *Regulating the Market for Snitches*, 47 BUFF. L. REV. 563, 564–65 (1999); Mark Curriden, *The Informant Trap: Secret Threat to Justice*, NAT. L.J., Feb. 20, 1995, at A1.

147. See Natapoff, *supra* note 146, at 675 n. 140 (emphasizing that in the majority of cases surveyed "courts find that informant activities take place at arms length from government handlers and therefore do not qualify as state action"). *But see* *Arizona v. Fulminante*, 499 U.S. 279, 287–88 (1991) (finding a jailhouse informant working with FBI to have engineered a coerced confession).

148. Curriden, *supra* note 146.

149. See Natapoff, *supra* note 146, at 653.

150. See Adrian Vermeule, *Emergency Lawmaking After 9/11 and 7/7*, 75 U. CHI. L. REV. 1155, 1164, 1175–76 (2008) (emphasizing that lawmakers faced with the uncertainties associated with still-evolving emergencies cannot foresee how events will unfold and thus tend to give the Executive broad, open-ended discretion and flexibility to confront both likely and unexpected challenges).

151. See *CIA v. Sims*, 471 U.S. 154, 167 (1985) (describing "sources and methods" as the "heart of all intelligence operations"); *Webster v. Doe*, 486 U.S. 592, 604 (1988) (noting the extraordinary need in the intelligence context "for confidentiality and the protection of . . . methods, sources, and mission").

legal authority—proceeded to request, pressure, and conscript America’s bankers to help stabilize the markets in a variety of ways.¹⁵² The government officials struck deals,¹⁵³ engaging in freewheeling negotiations, exacting concessions, and conditioning government bailouts on managerial control (or input in executive decisions), all the while emphasizing the need for firms to think beyond the immediate financial interests of their specific principals and work generally to avoid economic chaos and panic.¹⁵⁴ Whereas the deputization here looks quite different from what we see in the counterterrorism and law enforcement contexts, this is another manifestation of private–public regulation and coordinated action outside the scope of traditional administrative law or contractual channels.¹⁵⁵ The legal uncertainties,¹⁵⁶ the demands of crisis management,¹⁵⁷ the procedural informality associated with how the government approaches various private actors,¹⁵⁸ and the market distortions that might be generated (even if the distortions are “corrective”)¹⁵⁹ all suggest an important linkage in terms of the benefits and challenges of private–public partnerships hatched on the fly. More problematic in this context than perhaps others, the ad hoc negotiations might be viewed as especially disconcerting given the appearance of

152. See James B. Stewart, *Eight Days: The Battle To Save the American Financial System*, NEW YORKER, Sept. 21, 2009, at 59, 67–68 (describing pressure the SEC and Treasury placed on Lehman Brothers regarding the timing of its bankruptcy filing); see also Ben Hallman, *A Moment’s Notice for Lehman*, AM. LAW., Dec. 1, 2008, at 87, 88 (reporting that government officials urged Lehman Brothers to file for bankruptcy protection at a specific time because it was a “critical part of a program [the government] wanted to roll out”).

153. See Steven Davidoff & David Zaring, *Regulation by Deal*, 61 ADMIN. L. REV. 463, 466–68, 493–512 (2009).

154. See ANDREW ROSS SORKIN, TOO BIG TO FAIL 401–03 (2009) (noting the government’s demand that AIG executives resign as a condition of the federal government bailing out the company); James Bandler, *Hank’s Last Stand*, FORTUNE, Oct. 7, 2008, at 112. See generally U.S. GOV’T ACCOUNTABILITY OFFICE, TROUBLED ASSET RELIEF PROGRAM: THE U.S. GOVERNMENT ROLE AS SHAREHOLDER IN AIG, CITIGROUP, CHRYSLER, AND GENERAL MOTORS AND PRELIMINARY VIEWS ON ITS INVESTMENT MANAGEMENT ACTIVITIES 10–15 (2009) (describing the government’s management of its equity stakes in bailed-out corporations).

155. See Davidoff & Zaring, *supra* note 153, at 468 (“[T]he government structured deals that pushed its legal authority to the very edge and beyond in pursuit of, and bound by, its own political, economic, and, perhaps, sociological interests.”); *id.* at 535–36 (noting the government’s departure from traditional administrative law practices throughout the financial-crisis negotiations).

156. See *id.* at 468. But see Eric A. Posner & Adrian Vermeule, *Crisis Governance in the Administrative State: 9/11 and the Financial Meltdown of 2008*, 76 U. CHI. L. REV. 1613, 1638 (2009) (noting that the bailouts were rendered pursuant to existing statutory authority for the government to extend loans to institutions “whose failure threatens the health of the financial system”).

157. See generally Posner & Vermeule, *supra* note 156.

158. See Stewart, *supra* note 152, at 72; see also Richard W. Painter, *Bailouts: An Essay on Conflicts of Interest and Ethics when Government Pays the Tab*, 41 MCGEORGE L. REV. 131, 142 (2009) (characterizing “[t]he apparent arbitrariness of bailout decisions in 2008 and 2009”).

159. See Brady Dennis, *Fed Criticized for Not Negotiating Harder with AIG*, WASH. POST, Nov. 17, 2009, at A24; Joe Nocera, *Lehman Had To Die, It Seems, So Global Finance Could Live*, N.Y. TIMES, Sept. 12, 2009, at A1 (noting the apparent dissimilar treatment Lehman Brothers received vis-à-vis other firms that the government helped prop up).

conflicts of interest between high-ranking government officials and the private financial institutions, firms where some of the chief government decisionmakers previously worked and where they might seek employment after completing their public service.¹⁶⁰

B. *Legal Certainty's Challenges*

Second, though legal uncertainty introduces or exacerbates the challenges considered in Part II, it is not clear that the converse—legal certainty—would necessarily be a categorical improvement. Some of the uncertainty that attaches to a regime of unregulated or underregulated practices in homeland security is inevitable. After all, we might be hard-pressed to design a system that creates a *third* legal regime (i.e., neither private nor state actor) for all deputies, across the board. Such a system might make sense with respect to telecom workers essentially embedded with the FBI on long-term assignments,¹⁶¹ but not vis-à-vis, say, deputized truckers, any one of whom will, in all likelihood, never actually witness a terrorism-related suspicious activity. Moreover, whatever this third, hybrid regime might look like for deputies facilitating government operations, it would assuredly create new line-drawing problems, even if it were to resolve the ones discussed in Part II.

Nor would a system that imposed greater legal requirements on the private sector necessarily be welcomed (even if it is clarifying). For instance, the non-statutory, ostensibly voluntary practices described above permit deputies a modicum of choice in terms of whether and how to participate. This is true especially where the government isn't applying coercive pressure on would-be deputies to get involved. Where partnerships are open-ended and voluntary, the deputies likely view their efforts as public service rather than regulatory conscription. That service orientation might be considerably more civically meaningful, and politically legitimate, to the participants.¹⁶² In addition, legislation and regulatory rules are sticky. There

160. See Painter, *supra* note 158, at 140–42 (describing widespread appearances of conflicts of interest); Jim Puzzanghera, *Paulson Takes Heat for Role in Bailouts*, L.A. TIMES, July 17, 2009, at B1 (quoting a member of Congress accusing former-Treasury Secretary Paulson of taking \$700 billion and “giv[ing] it to [his] pals”); Andrew Ross Sorkin, *Paulson's Calls to Goldman May Have Tested Ethics*, N.Y. TIMES.COM, Aug. 10, 2009, <http://dealbook.blogs.nytimes.com/2009/08/10/paulsons-calls-to-goldman-tested-ethics/> (noting that questions are still being raised about then-Secretary Paulson's participation in decisions “to prop up the teetering financial system with tens of billions of taxpayer dollars, including aid that directly benefited his former firm”).

161. Cf. *supra* subpart I(B) (describing long-term, institutionalized deputization relationships between the telecoms and the government).

162. Cf. Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 54 (1997) (describing the advantages of labor agreements reached through consensus, as opposed to judicial or agency decree); Philip J. Harter, *Negotiating Regulations: A Cure for the Malaise*, 71 GEO. L.J. 1, 31 (1981) (advocating the use of negotiation in rulemaking because, among other reasons, it adds legitimacy and interest-group “buy in”); Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L.

is the often-voiced complaint that measures enacted during times of emergency are difficult to get off the books, even after the crisis abates. Their effective permanence thus contributes to a one-way ratchet of security measures that persist long beyond the period for which they are needed (and are themselves then augmented when a new threat arises).¹⁶³ On the other hand, practices not ossified via statutes and rules might be subject to more rapid termination once the need for private assistance lessens.¹⁶⁴

C. *Distinguishing Acceptable from Unacceptable Deputization Practices*

These claims about the potential limitations associated with certainty are not advanced to promote or endorse a brand of purposive uncertainty; rather, they are advanced simply to acknowledge that the (perhaps) intuitively attractive alternative might carry with it no shortage of its own baggage. These claims, coupled with the recognition that deputization implicates policy space far broader than just post-9/11 homeland security efforts, take us to the third discussion: we need to do more careful thinking about the nature of ad hoc deputization arrangements to gauge where they ought to be allowed to continue unaltered (notwithstanding the concomitant legal uncertainties) and where they should be harnessed within a regulatory framework that has a stronger legal foundation. That is a big project, and any comprehensive treatment is beyond the scope of this contribution. Here, however, I will provide preliminary thoughts on how we might go about distinguishing between acceptable and unacceptable deputization practices.

The discussion in Part I, highlighting differences between employee and organizational assistance, provides us with some clues, as do the assessments of the challenges identified in Part II. In thinking more broadly, we might want to build on those understandings, among others, and consider the acceptability of unregulated or underregulated deputization along three

REV. 342, 371–404 (2004) (describing a shift in regulatory governance toward a more participatory, collaborative, and flexible decisionmaking model).

163. See BRUCE ACKERMAN, *BEFORE THE NEXT ATTACK: PRESERVING CIVIL LIBERTIES IN AN AGE OF TERRORISM* 2–3 (2006) (noting that emergency measures enacted during a crisis are often not repealed after the crisis abates and indicating that those measures are further supplemented by an additional wave of emergency authorizations when a new crisis arises); Oren Gross, *Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?*, 112 YALE L.J. 1011, 1090 (2003) (“It is commonplace to find on statute books legislative acts that had originally been enacted as temporary emergency or counterterrorism measures, but that were subsequently transformed into permanent legislation.”); *id.* at 1095–96 (describing the ratcheting up of emergency powers as new crises arise); Jules Lobel, *Emergency Power and the Decline of Liberalism*, 98 YALE L.J. 1385, 1397–1421 (1989). *But see* Eric A. Posner & Adrian Vermeule, *Accommodating Emergencies*, 56 STAN. L. REV. 605, 610–26 (2003) (questioning the ratchet theory).

164. Indeed, even if government officials are not inclined to decrease the scope or intensity of operations when the circumstances seem objectively to warrant such downscaling, the private partners might serve as an independent check—refusing to cooperate, or limiting their cooperation, in light of the changed (and seemingly less dire) circumstances. Needless to note, this check is hardly perfect. Among other things, the private partners are not in the best position to make assessments regarding the relevant threats facing the United States.

planes: (1) the interests served by the government's preference for deputization over more conventional, legally grounded forms of private-public cooperation; (2) the compatibility or consistency of the deputization project (and the concomitant legal uncertainties that go along with it) with preexisting legal and institutional norms and understandings; and, (3) the tangible and distributional effects of the deputization arrangements.

With respect to the interests promoted by the government's preference for unregulated or underregulated collaborations, the question is whether an ad hoc arrangement is pursued because it is the most feasible way to proceed, because it is easier than adhering to the alternative, but *feasible*, legal protocols (e.g., warrants, subpoenas, contracts, or regulatory directives), or because proceeding in such a fashion confers an otherwise unobtainable legal advantage to carry out an assignment. Admittedly, there likely will be times when "most feasible" and "easier" blend together, and times when "easier" seems little more than a euphemism for "circumventing the law." Admittedly, too, the prospect of making objective determinations as to what is driving an arrangement is a daunting one. But for purposes of this initial sketch, we can leave those complications to the side and consider the legitimacy of a deputization program as a function of whether the non-statutory, non-regulatory arrangement is practical, reasonable, and perhaps necessary, or whether it is structured that way to enable an apparent power grab.¹⁶⁵

With respect to the issue of fidelity to or consistency with preexisting understandings, the question is how much of a departure are the deputies' roles—vis-à-vis both the government and their commercial clients—from those the corporations and corporate employees played prior to entering into the hybridized space. In other words, what were the legal and social expectations absent deputization? For instance, some private actors already have preexisting relationships with law enforcement, relationships that stem from legal requirements or professional obligations.¹⁶⁶ Duties of certain medical professionals to report instances of suspected domestic violence¹⁶⁷ or of lawyers and psychologists to take steps if they think their clients are about to commit violent acts come to mind as some additional examples.¹⁶⁸ By

165. I address similar questions with respect to privatization and the contracting out of government responsibilities in Michaels, *supra* note 20.

166. See, e.g., Bank Secrecy Act of 1970, 31 U.S.C. §§ 5311–5330 (2006) (requiring banks to maintain specific records for use in criminal, tax, and regulatory investigations and proceedings and to file Suspicious Activity Reports, or SARs).

167. See, e.g., Lois A. Weithorn, *Protecting Children from Exposure to Domestic Violence: The Use and Abuse of Child Maltreatment Statutes*, 53 HASTINGS L.J. 1, 28 (2001) (referencing various reporting requirements for medical personnel).

168. See *Tarasoff v. Regents of Univ. of Cal.*, 551 P.2d 334, 348 (Cal. 1976) (acknowledging affirmative duties for mental-health practitioners to recognize patients' violent inclinations and to take steps to prevent the patients from acting on those inclinations); MODEL CODE OF PROF'L RESPONSIBILITY DR 4-101(C) (1980) (permitting attorney disclosure of confidential communications with a client in order to help prevent crime); see also Stephen Gillers, *A Duty To Warn*, N.Y. TIMES, July 26, 2001, at A25.

contrast, the baseline understandings regarding the professional and legal duties imposed on (or embraced by) service technicians or building supervisors upon entering the homes of their customers or tenants might be very different.¹⁶⁹ Moreover, where government interactions with certain industries are already relatively free-wheeling and informal (on matters, say, of domestic regulation), opting for homeland security deputization arrangements over statutory or regulatory means of compelling assistance might make considerable sense; where government-industry interactions have largely been at arm's length, however, the introduction of informal homeland security deputization protocols might be quite a departure from past practices. In addition, if firms or industries have a track record of informing their customers in accessible and transparent ways that their privacy is not being safeguarded, that too would suggest less confusion or opportunity for novel exploitation if and when those firms assume roles as full-fledged deputies. Finally, if a deputization relationship were publicly announced—rather than hashed out in secret behind closed doors—even though the deputization program may traffic in legal uncertainties on the ground, there would be a modicum of notice alerting customers (not to mention legislators and judges, too) to adjust to the ensuing practices accordingly. If, on the other hand, deputization appears to be a stark reversal, and undertaken without any public disclosure acknowledging and giving advanced warning of the shift,¹⁷⁰ that might be a basis for looking at the arrangements with greater skepticism, perhaps with a view to impose requirements that increase everyone's legal certainty regarding the relevant practices.

With respect to concerns about deputization's effects on, among other things, homeland security, civil liberties, and private industry, an accounting of the potency of the programs is in order. Potency could be a function of the number of deputies mobilized, and the invasiveness of deputies' reach (in terms of physical space and aggregation of data). Potency might (also or alternatively) reflect the market distortions deputization engenders. Arrangements that turn on coercive, unregulated interactions with firms or industries might invite greater scrutiny than those collaborations that truly are voluntary in nature. Further, a program's potency might be measured in terms of the potential for deputies to act abusively in a given arrangement—and thus be inversely related to how much control the government can exert over their private partners to keep them in line.

This rough sketch cannot fully do justice to the detailed analysis that is required to map out the private-public collaborations along axes that would

169. See *supra* note 18 and accompanying text.

170. See, e.g., *AT&T Revises Privacy Policy for Customer Data*, N.Y. TIMES, June 22, 2006, at C7; Barbara Ortutay, Associated Press, *Facebook Backtracks on Terms of Use After Protests*, LAW.COM, Feb. 18, 2009, <http://www.law.com/jsp/article.jsp?id=1202428366838> (describing strong opposition mounted by Facebook users after the social networking site sought to make unilateral and retroactively applicable changes to its user privacy policies).

inform whether regulatory interventions would be helpful in addressing, among other things, exploitative, undemocratic, and counterproductive practices in legally ambiguous deputized space. Nor does it provide foundational benchmarks that would ensure that this scrutiny is not simply ad hoc review of ad hoc arrangements.¹⁷¹ That said, this sketch offers some analytical and normative tools for recognizing the diversity of deputization practices and thinking carefully about such interventions, principally in the context of homeland security but perhaps more broadly as well. By way of conclusion, as we approach the second decade of what is popularly termed the Global War on Terror, one hopes that this and the related contributions to this Symposium will spark continued debate and further research to address the institutional challenges brought about in the course of mobilizing an effective response to the terrorist threat.

171. Most balancing tests are susceptible to such claims—levied perhaps most forcefully by Justice Scalia—that they are unprincipled and results oriented. See, e.g., *Morrison v. Olson*, 487 U.S. 654, 734 (1988) (Scalia, J., dissenting) (arguing that the “‘totality of the circumstances’ mode of analysis . . . is . . . guaranteed to produce a result, in every case, that will make a majority of the Court happy with the law. The law is, by definition, precisely what the majority thinks, taking all things into account, it *ought* to be”); *United States v. Mead*, 533 U.S. 218, 241 (2001) (Scalia, J., dissenting) (describing “th’ol’ ‘totality of the circumstances’ test” as the “test most beloved by a court unwilling to be held to rules (and most feared by litigants who want to know what to expect)”). While not unpersuasive, the fact of the matter is that the landscape for deputization is quite varied and whatever benefits accompany bright-line rules are more than overshadowed by the costs such an inflexible approach would impose on policymakers or judges. Indeed, the rejoinder to Justice Scalia’s broadside in *Mead* is instructive. In noting the diversity of authorized agency activity (ranging from formal adjudication to informal opinion letters), the Court rejected Justice Scalia’s *either-or* approach whether to defer to agency interpretations of statutory authority. *Id.* at 235–37. Instead it accepted the patchwork of regulatory actors and activities involved in statutory interpretation and acknowledged that a broad array of factors must be considered in developing a coherent understanding of where—and to what degree—deference ought to be accorded. See *id.* Unless one takes a categorical approach in support of or entirely against a similarly diverse range of deputization arrangements operating in the interstices of the law, then a more nuanced, albeit at times unwieldy, totality-like metric appears warranted here.

The Case for Stewart over Harlan on 24/7 Physical Surveillance

Afsheen John Radsan*

I. Introduction

My premise is that the government's physical surveillance can reach a point in terms of duration and intensity that it becomes a "search" under the Fourth Amendment. If one accepts the common sense of this premise, the law of surveillance should change. The changes can come from the Executive branch by orders, regulations, or guidelines; from Congress by a statute that gives citizens more protections from governmental intrusions than the courts have given so far; or from the courts by new holdings that do a better job of balancing individual freedom against the government's duty to protect us from dangers, including terrorist attacks.

If, by doctrinal change, some types of physical surveillance are accepted as a search, subsidiary questions present themselves. Is a warrant required? Probable cause? Reasonable suspicion? Or is an even lower standard possible that recognizes that terrorism cases are significantly different from ordinary cases? If individual suspicion is not there, the government might attempt to justify a search through some "special need." But arguing for a special need (say, in a sobriety checkpoint) is quite different in doctrinal terms from arguing that a search did not occur at all (say, in a canine sniff of a piece of luggage).¹ This Article, while not indifferent to these subsidiary questions, does not specify the appropriate level of suspicion for pervasive, physical surveillance. Nor does it apply the proposed framework to rework all Supreme Court cases since 1967 on what constitutes a search. Instead, this Article examines just one area of Fourth Amendment jurisprudence through the dark lens of 9/11.

In helping to answer when governmental action becomes a search, *Katz v. United States*² and *Kyllo v. United States*³ stand out from the canon. Depending on one's point of view, *Kyllo* may be the last case from the *Katz* era

* Professor of Law, William Mitchell College of Law. Professor Radsan is a former federal prosecutor. He thanks Adam Pabarcus, Christopher Proczko, and Dan Ryan for their outstanding research assistance.

1. Compare Andrea J. Cook, *Sobriety Checkpoints Deter Drunken Drivers*, RAPID CITY J., Mar. 15, 2010, available at http://www.rapidcityjournal.com/news/article_02ab6a3c-2fdc-11df-b99d-001cc4c03286.html (discussing the implementation and effectiveness of sobriety checkpoints), with David G. Savage, *High Court to Rule on 'Canine Sniff' Search*, L.A. TIMES, Apr. 6, 2004, available at <http://articles.latimes.com/2004/apr/06/nation/na-scotus6> (discussing a case in which prosecutors argued that a dog sniffing the air does not amount to a search).

2. 389 U.S. 347 (1967).

3. 533 U.S. 27 (2001).

or the first case from a new era. *Katz*, decided in 1967, swept away a prior emphasis on property rights and trespass laws to hold that the electronic monitoring of a phone booth was a search.⁴ Since then, the two-part test from Justice Harlan's concurring opinion has received as much attention as the totality-of-the-circumstances test in Justice Stewart's majority opinion.⁵ *Kyllo*, decided just months before 9/11, ruled that the government's use of a thermal-imaging device from outside a house was a search.⁶ For the era after 9/11, a blend of Justice Harlan's test in *Katz* with Justice Scalia's opinion in *Kyllo* reproduces Justice Stewart's test, a more open-ended test which makes room for property, liberty, secrecy, anonymity, autonomy, and privacy, as well as other values that may undergird the "right of the people to be secure in their persons, houses, papers, and effects."⁷ Justice Stewart's test helps not only on one issue of physical surveillance but also opens up new approaches to data mining and other Fourth Amendment issues at the intersection of national security, privacy, and technology.

II. Implications of Another Terrorist Attack

Before the next terrorist attack—and the ensuing panic that will make civil-libertarian proposals even more difficult to achieve⁸—I challenge the consensus that all physical surveillance falls outside the Fourth Amendment.⁹ For these purposes, I limit my analysis to trends in the courts and in academic commentary since 9/11. A sympathetic reader might accept this limitation for at least two reasons. First, the space for a symposium piece does not permit an extensive review of related Fourth Amendment topics:

4. See *Katz*, 389 U.S. at 353 (holding that electronic monitoring of a telephone booth violated the Fourth Amendment, despite the lack of physical intrusion into the booth).

5. See, e.g., Clark D. Cunningham, *A Linguistic Analysis of the Meanings of "Search" in the Fourth Amendment: A Search for Common Sense*, 73 IOWA L. REV. 541, 568 (1988) (noting that the result in *Katz* derived from Harlan's concurrence is "universally praised while the majority opinion either is ignored or deprecated").

6. *Kyllo*, 533 U.S. at 34 ("[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use." (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961))).

7. U.S. CONST. amend. IV. See generally Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994) (arguing that Fourth Amendment searches should be judged not by the Supreme Court's confused and confusing doctrine but by their reasonableness).

8. See, e.g., BRUCE ACKERMAN, *BEFORE THE NEXT ATTACK 2* (2006) (predicting that successful terrorist attacks will result in a proliferation of repressive laws undercutting civil liberties).

9. See Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 381 (1974) (explaining that the "maxim that the eye or ear could not commit a search" traces "back to English common law and had been mentioned by Lord Camden in his celebrated judgment in *Entick v. Carrington*, which has always been justly received as something of a lexicon of the 'original understanding' of the fourth amendment.").

open fields,¹⁰ curtilage,¹¹ garbage bags,¹² pen registers,¹³ and dog sniffs.¹⁴ Second, any conclusions from before 9/11 may not properly factor into the equation the very real possibility of the next catastrophic attack; 9/11, a dividing line between eras, continues as a major marker in policy making and legal analysis.

Definitions are important. My use of the term “physical surveillance” attempts to separate this analysis from an analysis of “electronic surveillance.” The attempted distinction is between FBI agents on the street and National Security Agency computers that suck in e-mail, telephone, and other signals. But physical surveillance is also a bit of a misnomer. FBI agents do not usually seek to make physical contact with their suspects during surveillance; in many cases, the FBI does not want the suspects to know they are being observed.¹⁵ Watching from the shadows, the FBI hopes suspected bad guys will take the FBI to other bad guys.¹⁶ So this sort of surveillance might also be called “visual surveillance.”

Imagine teams of FBI agents following a suspected terrorist in New York City. A team in the lobby across the street watches the suspect leave his apartment on the Upper West Side. They take photographs. Another team joins him on the Number One subway headed downtown. Several teams watch the entrances to 125 Broad Street, the downtown building where the suspect has an office. They use binoculars. Hours go by. Another team tails the suspect by car as he rides out of the garage, driven by another person toward Newark. Helicopters and planes assist the agents on the ground. A command post at FBI headquarters guides their action. Although the agents do not develop enough information for an arrest, they continue to be

10. See, e.g., David E. Steinberg, *The Original Understanding of Unreasonable Searches and Seizures*, 56 FLA. L. REV. 1051, 1058–59 (2004) (discussing the Supreme Court’s holding that the Fourth Amendment does not apply to police searches in open fields).

11. See, e.g., Catherine Hancock, *Justice Powell’s Garden: The Ciraolo Dissent and Fourth Amendment Protection for Curtilage-Home Privacy*, 44 SAN DIEGO L. REV. 551, 559–65 (2007) (describing the Supreme Court’s treatment in *Ciraolo* of pre-*Katz* curtilage doctrines).

12. See, e.g., Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 616–24 (1989) (discussing the Supreme Court’s holding in *California v. Greenwood*, 486 U.S. 35 (1988), that property owners have no subjective expectation of privacy in their garbage that society would accept as “objectively reasonable”).

13. See, e.g., Paul M. Schwartz, *Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes’s Jorde Lecture*, 97 CAL. L. REV. 407, 427–28 (2009) (lamenting the lack of pen-register reports by Congress as authorized by the Pen Register Act).

14. See Savage, *supra* note 1 (discussing a case in which prosecutors argued that a dog sniffing the air does not amount to a search).

15. See *Weekend Edition Saturday: FBI Surveillance Team Reveals Tricks of the Trade* (NPR radio broadcast July 5, 2008), available at <http://www.npr.org/templates/transcript/transcript.php?storyId=92207687> (describing a variety of FBI surveillance techniques designed to ensure that suspects are unaware of the FBI’s presence).

16. See *Talk of the Nation: How to Prevent Home Grown Terrorism* (NPR radio broadcast Dec. 15, 2009), available at <http://www.npr.org/templates/story/story.php?storyId=121473067> (proclaiming that one of the main goals of surveillance is to find other people to further the investigation).

suspicious based on their read of the suspect and on tips from the Intelligence Community. The FBI is not allowed to use these tips in a search warrant, however, because the Intelligence Community insists on full protection for its sources and methods as the price for its cooperation on this case. Not sure what else to do, the FBI adds teams and resources. In early September, the suspect, backing up on the sidewalk and looking into shop windows on Columbus Avenue, spots the surveillance. The original operation is blown.

Next, as a sort of deterrence, the FBI agents decide to make the surveillance even more visible to the suspect. Everywhere the suspect goes, he knows he is being watched: at home, at work, and in the coffee shop where he smokes a water pipe with friends. His family and friends also see that he is being watched. The surveillance goes on for months. It is expensive—and often boring for the agents. If the law made sense then this sort of open, pervasive physical surveillance would fall under the Fourth Amendment.¹⁷ Unfortunately for the suspect, Fourth Amendment law is not always rational. And the line between investigation and harassment is not always clear.

Terrorism investigations can go from boring to exciting in the click of a trigger. Imagine that the suspect eludes FBI surveillance, and on September 12, 2011, a synchronized set of bombings goes off around the United States. From 8:00 a.m. until 8:30 a.m., in fifteen-minute intervals, the New York subway system, the Washington, D.C. Metro, and the Chicago L are all attacked. The timing and sophistication of the attacks carry al Qaeda's evil signs. The bombs, detonated by cell phones, were contained in backpacks left on the trains. Hundreds are dead, thousands wounded. Panic has set in, and the American public wants the government to do what is necessary for them to feel safe again. In response, government agents are everywhere. The physical surveillance is more intense than after 9/11. The agents on the streets of American cities look like soldiers on battlefields in Afghanistan. They carry machine guns and wear pistols in holsters. On their helmets are swiveling cameras that feed into an elaborate closed-circuit television system; controllers in the FBI's operations center can thus see the scene from the agents' perspectives. The agents see the world through specialized goggles, even more advanced than the infrared devices used by soldiers in Afghanistan. The new goggles, more penetrating than the scanners in security lines at American airports, allow the agents to see through people's clothes and skin for signs of hidden weapons. The frantic agents fear something much worse than the initial attack. With hand-held radiation detectors, far more sophisticated than Geiger counters from days gone by,

17. The text of the Amendment does not limit its application to clandestine searches and seizures. See U.S. CONST. amend. IV (preventing the government from violating the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures").

they look for signs that al Qaeda has smuggled a real nuclear weapon into an American city.

Neither this scenario nor the use of technology is far-fetched. Cameras, infrared goggles, and radiation detectors are part of governmental arsenals.¹⁸ These technologies can easily be adjusted and combined for law enforcement purposes.

Across the Atlantic, British residents are accustomed to pervasive CCTV.¹⁹ A ride on a bicycle from Hampstead Heath to Hyde Park is recorded by hundreds, if not thousands, of cameras.²⁰ These cameras feed into command centers around the city.²¹ In this area of government intrusion, the British public seems more resigned than the American public to losses in their privacy. Having endured a time of troubles when the IRA regularly bombed targets, the British lost their innocence long before 9/11.²² Thus, Americans may be catching up to their British cousins on CCTV.

On traditional battlefields, the American soldier's use of infrared goggles gives him a distinct advantage over enemies whose gear is less advanced. At times, the American can literally see through walls,²³ and fighting after the sun has set is still possible because he can see through the blackness of night.²⁴ Military technologies, of course, often lead to civilian variations.²⁵

Radiation detectors were visible to some people in American cities after 9/11.²⁶ Whether the American government acknowledged the specifics or not, any driver heading into Washington, D.C., could easily project an official purpose onto the cables and cords strapped down to main roads and attached to black boxes. Many drivers may have assumed the plain vans in

18. See, e.g., Richard A. Serrano, *FBI Monitors for Radiation at Some Mosques*, L.A. TIMES, Dec. 24, 2005, at A16 (asserting that "investigators used special equipment to gauge radiation levels at homes, businesses, warehouses and centers of some Muslim groups").

19. See, e.g., Helen Carter & David Ward, *CCTV Captures a Boy on a Bike—Thirty Seconds Later He Had Killed Rhys Jones*, GUARDIAN, Sept. 27, 2007, <http://www.guardian.co.uk/uk/2007/sep/27/topstories3.ukguns> (describing CCTV's role in a murder investigation in Liverpool and calls to enhance the system).

20. See Louise Osborne, *Hundreds of CCTV Cameras Watch Surrey Boroughs*, GET SURREY, Aug. 24, 2009, http://www.getsurrey.co.uk/news/s/2056165_hundreds_of_cctv_cameras_watch_surrey_boroughs (revealing that one small borough in England added 493 surveillance cameras over a one-year period).

21. See Chiltern Dist. Council, *How Does the CCTV Work?*, http://www.chiltern.gov.uk/site/scripts/documents_info.php?documentID=57&pageNumber=3 ("Specially trained staff monitor the CCTV pictures in a secure control room in High Wycombe.").

22. See STEVE HEWITT, *THE BRITISH WAR ON TERROR 9–28* (2008) (chronicling the British history with terrorism, focusing on violence with Ireland).

23. See ROBERT L. SNOW, *TECHNOLOGY AND LAW ENFORCEMENT 90* (2007) ("[S]everal manufacturers have developed portable, handheld devices that can see through . . . walls and detect motion on the other side.").

24. See *id.* (describing a "flashlight that illuminates the area with infrared radiation, allowing police officers with infrared sensing devices to see clearly in darkened areas").

25. See *id.* (noting that local law enforcement now uses sophisticated technology).

26. *Id.* at 68.

traffic contained even more sophisticated devices to detect biological, chemical, and nuclear weapons. As a faithful former public servant, I neither confirm nor deny.

The use of cameras, goggles, and radiation detectors may increase the government's chances of detecting terrorist plots. But, in a sort of boomerang, their pervasive use, much like the national threat levels perpetually at orange and red, may contribute to the fear that is the terrorist's goal. Whether they are used in the nation's counterterrorism arsenal has as much to do with politics as it does with law. The political calculations after the next attack, no doubt, may be much different from the calculations during the long lull in the homeland. Let us hope this lull lasts. And let us put some reasonable rules in place in advance.

III. The Legal Framework of Fourth Amendment Searches

A. *The Supreme Court*

Two Supreme Court cases, *Katz* and *Kyllo*, are important in determining whether simple or sophisticated surveillance constitutes a search. *Katz v. United States*, decided before the age of terror, was an important shift in the Court's analysis of the Fourth Amendment. Justice Stewart, writing for the Court, made clear the Court's rejection of a prior emphasis on physical trespass: "Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."²⁷ Justice Stewart decided that the government's listening to and recording of calls in a phone booth was a search that required a judicial warrant, something the government had not obtained.²⁸ He emphasized the importance of a neutral magistrate in authorizing searches as much as the notion that the Fourth Amendment did not always depend on trespass.²⁹ In reaching his conclusion, Justice Stewart did not present a list of factors—or that much analysis: "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."³⁰ Thus, the "public" phone booth played an important role in "private" communications. Overall, Justice Stewart tried to distinguish between what a person "knowingly exposes to the public" and what "he seeks to preserve as private."³¹

27. *Katz v. United States*, 389 U.S. 347, 353 (1967).

28. *Id.*

29. *Id.* at 354–55.

30. *Id.* at 353.

31. *Id.* at 351.

Academics and other judges might criticize Justice Stewart for not saying more on what made the government activity in *Katz* a search. Wiser commentators might see that Justice Stewart realized that some concepts such as “beyond a reasonable doubt” or “reasonable care” do not lend themselves to precision. Indeed, the attempt at too much precision or the use of multi-factored tests might actually undercut the conclusion. Much like the time when he knew “obscenity” when he saw it,³² perhaps Justice Stewart just knew a search when he saw it.

Justice Stewart’s rejection of prior cases and his reformulation of the term “search” opened up the Fourth Amendment to electronic surveillance. This decision was part of the package that prodded Congress into regulating electronic surveillance.³³ Title III³⁴ became the reference for law enforcement searches, and the Foreign Intelligence Surveillance Act³⁵ became the reference for national-security searches within the United States.

From *Katz*, Justice Harlan’s concurring opinion is remembered more than Justice Stewart’s opinion for the Court. Justice Harlan questioned whether the distinction between “people” and “places” was very clear.³⁶ Reference to a place is usually necessary, he believed, in determining whether a person has a constitutionally protected expectation of privacy.³⁷ For Justice Harlan, the telephone booth was a “temporarily private place whose momentary occupants’ expectations of freedom from intrusion are recognized as reasonable.”³⁸ So not only did Justice Harlan blur the distinction between people and places, but he also blurred the difference between public and private spaces. More famously, he offered a two-part test in determining whether a governmental search had occurred: “[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”³⁹ This test, as explained below, has found some favor in the

32. *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964) (Stewart, J., concurring) (“I shall not today attempt further to define the kinds of material I understand to be [hard-core pornography]; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it, and the motion picture involved in this case is not that.”).

33. See Tara Mikkilineni, Note, *Constitutional Default Rules and Interbranch Cooperation*, 82 N.Y.U. L. REV. 1403, 1411 (2007) (asserting that the Court’s decisions in *Katz* and *Berger v. New York*, 388 U.S. 41 (1967), “both led Congress to regulate electronic surveillance out of fear that the Court would otherwise ban the practice outright.”).

34. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801–804, 82 Stat. 197 (1968) (codified at 18 U.S.C. §§ 2510–2522 (2006)).

35. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered titles of U.S.C.).

36. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

37. *Id.*

38. *Id.*

39. *Id.*

lower courts.⁴⁰ Those who support Justice Harlan do not seem troubled that the second part of his test turns on the malleable term “reasonable.”

In *Kyllo v. United States*, the Supreme Court, in a 5–4 decision, decided that “the use of a thermal-imaging device aimed at a private home from a public street” constituted a search and therefore required a warrant.⁴¹ This case was decided a few months before 9/11, and it is quite possible that the case would have been decided differently if those attacks were factored into the Court’s calculations. For Justice Scalia, it was very important that the governmental activity was connected with the suspect’s home, a place of maximum constitutional protection from “prying government eyes.”⁴² While acknowledging that “visual” or “naked-eye” surveillance is generally not a search, Justice Scalia said *Kyllo* presented the question of “how much technological enhancement of ordinary perception, from such a vantage point, if any, is too much.”⁴³ In that regard, both the majority and the dissent in *Kyllo* devoted many more words to describing changes in technology than the *Katz* Court did. *Kyllo* was a decision for the wired age.

Justice Scalia saw the use of “sense-enhancing” technology as a search to the extent it revealed “details of the home that would previously have been unknowable without physical intrusion.”⁴⁴ Part of the pre-*Katz* era’s emphasis on trespass influenced his analysis. Reaching back to the eighteenth century, he noted “[v]isual surveillance was unquestionably lawful because ‘the eye cannot by the laws of England be guilty of a trespass.’”⁴⁵ Having separated Fourth Amendment rights from trespass and property law, the Court still preserved the possibility of “the lawfulness of warrantless visual surveillance of a home.”⁴⁶ Further, Justice Scalia rejected as unworkable any test that would require warrants for technological intrusions of the home only if they would reveal “intimate details.”⁴⁷ Because the sophistication of the technology has “no necessary connection . . . [to] the ‘intimacy’ of the details that it observes,”⁴⁸ such a distinction would give police officers no way “to know in advance whether [the search] is constitutional.”⁴⁹ Moreover, Justice Scalia determined that “[i]n the home . . . all details are intimate details.”⁵⁰ No matter how circular the *Katz* test may be, he maintained a bright line of

40. See *infra* section III(B)(1).

41. 533 U.S. 27, 29 (2001).

42. *Id.* at 37.

43. *Id.* at 33.

44. *Id.* at 40.

45. *Id.* at 31–32 (quoting *Boyd v. United States*, 116 U.S. 616, 628 (1886)).

46. *Id.* at 32.

47. *Id.* at 38.

48. *Id.*

49. *Id.* at 39 (emphasis omitted).

50. *Id.* at 37.

Fourth Amendment protection at the entrance of a home.⁵¹ Yet, insofar as his analysis depends on the technology not being in “general public use,”⁵² Justice Scalia’s protection may not be total. As Justice Stevens noted in dissent, “the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available.”⁵³

Justice Stevens, writing with ironical relish, accused Justice Scalia of judicial activism in *Kyllo*. Instead of trying “to craft an all-encompassing rule for the future,” Justice Stevens advised the Court “to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints.”⁵⁴ Justice Stevens did not believe the homeowner had a reasonable expectation of privacy in the mere “heat emissions” from his home.⁵⁵ In addition to heat emissions, Justice Stevens listed other things in the “public domain”: traces of smoke, suspicious odors, odorless gases, and airborne particulates.⁵⁶ Presaging the 9/11 era and the possible use of radiation detectors in this Article’s scenario, he also mentioned “radioactive emissions.”⁵⁷ For the most part, Justice Stevens’s argument is good for those who do not want any limits on physical surveillance. Because this sort of surveillance does not violate a reasonable expectation of privacy, Justice Stevens does not construe it as a search.⁵⁸ Government agents, for him, are free to observe people from places outside their homes.

Other than passing references from Supreme Court justices,⁵⁹ not much case law examines the limits of physical surveillance, before or after 9/11.⁶⁰ The subjects of the surveillance may not know what the government is doing, and if the government does not detain or arrest them, they will not be able to complain that the government’s conduct caused them any harm.⁶¹ If they are

51. Justice Scalia does not like the *Katz* test, even though he uses it to reach the same result. He suggests a return to an original definition of “search” as looking over or through something or exploring or examining. See *id.* at 32–33, 32 n.1 (citing N. WEBSTER, AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE 66 (6th ed. 1989) (1828)). He says that the Court “must take the long view, from the original meaning of the Fourth Amendment forward.” *Id.* at 40. Conceding “searches” in more cases, Justice Scalia would move the emphasis of the analysis to whether those governmental actions were “reasonable.” See Amar, *supra* note 7, at 760 n.4 (agreeing with Justice Scalia’s belief that reasonableness is the touchstone of the Fourteenth Amendment).

52. *Kyllo*, 533 U.S. at 40.

53. *Id.* at 47 (Stevens, J., dissenting).

54. *Id.* at 51.

55. *Id.* at 45.

56. *Id.*

57. *Id.*

58. *Id.* at 44.

59. See *id.* at 33–34 (declaring the difficulty of setting limits to physical surveillance as technology advances).

60. See Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association’s Tentative Draft Standards*, 10 HARV. J. L. & TECH. 383, 401–02 (lamenting that current case law leaves many issues with physical surveillance unaddressed).

61. See, e.g., *infra* subpart III(C).

detained or arrested, the government may find it easy under prevailing notions to demonstrate to a court that the physical surveillance did not constitute a search.⁶² Although the Supreme Court has not directly ruled on physical surveillance, its decisions, including *Kyllo*, take for granted that this type of governmental action is not a search.⁶³

In *United States v. Knotts*,⁶⁴ for example, the Supreme Court held that the government's installation and tracking of a radio beeper in a chemical drum was not a search.⁶⁵ To reach this result, the Court said that the beeper did not provide anything the police could not obtain—with more effort—through visual surveillance in public places.⁶⁶ The government tracked the drum between the chloroform's purchase in Minneapolis, Minnesota, and the defendant's cabin near Shell Lake, Wisconsin.⁶⁷ Thus, the tracking was not inside the defendant's home. Writing for the Court, Justice Rehnquist emphasized that this case was not about twenty-four-hour surveillance. As he said, "[I]f such dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."⁶⁸ Twenty-seven years later, the Supreme Court has still not returned to the issue which Rehnquist left open in *Knotts*: pervasive, physical surveillance.

B. *The Lower Courts*

The United States Supreme Court has not devoted many pages to "expectations of privacy" since 9/11.⁶⁹ Even its opinions related to the Fourth Amendment have been on other topics.⁷⁰ The lower courts, left alone,

62. See *infra* subpart III(C).

63. See *infra* notes 63–66 and accompanying text; cf. *California v. Ciraolo*, 476 U.S. 207, 213 (1986) (recognizing as legal under the Fourth Amendment an officer's observations of a suspect who knowingly exposes her activity to the public).

64. 460 U.S. 276 (1983).

65. *Id.* at 285.

66. *Id.* at 282.

67. *Id.* at 278.

68. *Id.* at 284.

69. See *supra* notes 59–60 and accompanying text.

70. See *Arizona v. Gant*, 129 S. Ct. 1710, 1716 (2009) (citing *Katz* to support the existence of exceptions to the warrant requirement) (holding that the exception that allows a warrantless search incident to arrest in a car applies only to the area in which the arrestee might grab a weapon or destroy evidence); *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006) (citing *Katz* to support exceptions to the warrant requirement) (holding that a police officer may enter a home without a warrant if he has an objectively reasonable basis to believe an occupant is seriously injured or faces imminent serious injury); *Georgia v. Randolph*, 547 U.S. 103, 110, 114 (2006) (using *Katz* in the majority to separate Fourth Amendment rights from property law; in dissent, citing Justice Harlan's *Katz* concurrence as the outside limit of the Court's inquiry into expectations of privacy) (holding that consent disputed by a physically present co-inhabitant is no exception to the warrant requirement); *United States v. Grubbs*, 547 U.S. 90, 95 (2006) (citing *Katz* as an example of anticipatory warrants in the context of electronic surveillance) (holding that anticipatory warrants do not violate Fourth Amendment rights and that the Fourth Amendment does not require an anticipatory warrant to list its triggering condition); *Illinois v. Caballes*, 543 U.S. 405, 416 n.6

continue to answer difficult questions of whether government conduct constitutes a search.⁷¹ My goal in surveying these decisions is to determine how faithful lower courts are in applying Harlan's two-part test and how useful those two parts are to their analysis. In the federal courts of appeals, there is a range of faithfulness to Harlan's two-pronged approach for determining whether government action rises to a search. Some courts apply Harlan by the book.⁷² Other courts apply some but not all of Harlan.⁷³ And still others ignore him, taking another approach.⁷⁴

1. *Application of Harlan*

a. Strict Adherence to Harlan's Test.—The federal courts of appeals that faithfully apply Harlan's test conduct a formal analysis of both prongs. The Seventh Circuit, for example, said the following in deciding whether police entry into the common area of a duplex was a search:

[Defendant] has not demonstrated a subjective expectation of privacy with respect to the common hallway. Nor has he shown that any subjectively held expectation of privacy that he might hold with respect to that hallway is one that society is prepared to recognize as reasonable Exposing the activities within the common hallway to the world is inconsistent with a subjective expectation of privacy

Even if [defendant] held a subjective expectation of privacy with respect to the common hallway, the facts of this case and our precedents reveal that such an expectation would not be "one that society is prepared to recognize as reasonable."⁷⁵

This is straight from Harlan.⁷⁶ Similarly, the Eleventh Circuit formally used both of Harlan's prongs. In *United States v. King*,⁷⁷ the defendant stored child pornography on a common network drive but took steps to secure access to his own computer.⁷⁸ The Court ruled that "[h]is experience

(2005) (citing *Katz* in dissent to demonstrate a manifestation of an expectation of privacy) (holding that a dog sniff around an automobile's exterior during a routine traffic stop does not require reasonable suspicion); *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (citing *Katz* for the necessity of magistrate-imposed restraint) (holding that a warrant that fails to describe the evidence sought is invalid and that a search pursuant to this warrant is unreasonable for lack of oversight by a magistrate).

71. See *infra* Part III.

72. See *infra* subsection III(B)(1)(a).

73. See *infra* subsection III(B)(1)(b).

74. See *infra* section III(B)(2).

75. *United States v. Villegas*, 495 F.3d 761, 767 (7th Cir. 2007) (quoting *United States v. Yang*, 478 F.3d 832, 835 (7th Cir. 2007)).

76. See *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

77. 509 F.3d 1338 (11th Cir. 2007).

78. *Id.* at 1339.

with computer security and the affirmative steps he took to install security settings demonstrate a subjective expectation of privacy in the files, so the question becomes ‘whether society is prepared to accept [King’s] subjective expectation of privacy as objectively reasonable.’”⁷⁹ Moving to the second prong, the court found that “[b]ecause his expectation of privacy was unreasonable King suffered no violation of his Fourth Amendment rights when his computer files were searched through the computer’s connection to the base network.”⁸⁰

The federal courts of appeals that faithfully and consistently adhere to Harlan are the Second,⁸¹ Seventh,⁸² Tenth,⁸³ Eleventh,⁸⁴ and the D.C.

79. *Id.* at 1341–42 (quoting *United States v. Hall*, 47 F.3d 1091, 1097 (11th Cir. 1995)).

80. *Id.* at 1342.

81. See *MacWade v. Kelly*, 460 F.3d 260, 272–73 (2d Cir. 2006) (holding that New York subway riders have a subjective expectation of privacy in the bags they carry into the subway, an expectation the Supreme Court has recognized as objectively reasonable); *United States v. Titemore*, 437 F.3d 251, 258 (2d Cir. 2006) (examining whether the defendant manifested a subjective expectation of privacy in part of a curtilage and whether society would recognize it as reasonable); *Palmieri v. Lynch*, 392 F.3d 73, 81 (2d Cir. 2004) (using the headings “subjective expectation of privacy” and “objectively reasonable expectation of privacy” for its analysis).

82. See *Michael C. v. Gresbach*, 526 F.3d 1008, 1015 (7th Cir. 2008) (“Private schools, by their very operation, exhibit a subjective expectation of privacy. . . . Moreover, an expectation of privacy is objectively reasonable where parents . . . expect that the parents’ express delegation of parental authority to school officials will be both acknowledged and respected by government actors.” (citations omitted)); *United States v. Figuero-Espana*, 511 F.3d 696, 704 (7th Cir. 2007) (“Without evidence suggesting that [he] was driving the truck with someone else’s permission, he cannot establish that he had a subjective expectation of privacy in the vehicle. Nor can he establish an objective expectation of privacy . . . [because he] failed to produce a valid driver’s license”); *United States v. Amaral-Estrada*, 509 F.3d 820, 827 (7th Cir. 2007) (reasoning that the defendant “failed to manifest any . . . actual or subjective expectation of privacy” in a vehicle he was borrowing and therefore did not exhibit any legitimate expectation of privacy); *Christensen v. County of Boone, Ill.*, 483 F.3d 454, 459–60 (7th Cir. 2007) (holding that there was no subjective or objectively reasonable expectation of privacy while driving on public streets or parking in a business parking lot); *United States v. Yang*, 478 F.3d 832, 836 (7th Cir. 2007) (“Because Yang had no subjective expectation of privacy in the notebooks, we need not reach the objectively reasonable injury.”); *United States v. Mendoza*, 438 F.3d 792, 795–96 (7th Cir. 2006) (analyzing the search of a garage through Harlan’s two-pronged test).

83. See *United States v. Worthon*, 520 F.3d 1173, 1182–83 (10th Cir. 2008) (“Mr. Romero unquestionably maintained no subjective expectation of privacy over the bags in the van. . . . [He also] made no showing that . . . would have allowed him to drive the car legitimately.” (quoting *United States v. Roper*, 918 F.2d 885, 887 (10th Cir. 1990))); *United States v. Barrows*, 481 F.3d 1246, 1248–49 (10th Cir. 2007) (holding that a personal computer Mr. Barrows brought to work from his home to use for common office functions may have established a subjective expectation of privacy, but not a reasonable expectation of privacy that society would recognize); *United States v. Hatfield*, 333 F.3d 1189, 1198 (10th Cir. 2003) (“Even though we can conclude that Hatfield had a subjective expectation of privacy in the space immediately behind his house, this is not an expectation of privacy that society regards as reasonable, at least with respect to visual observations made from an adjoining open field.”); *United States v. Rhiger*, 315 F.3d 1283, 1285–87 (10th Cir. 2003) (examining when a social guest establishes a subjective and legitimate expectation of privacy); *United States v. Higgins*, 282 F.3d 1261, 1272 (10th Cir. 2002) (“The facts that he had brought some personal property to the premises and that he had plans to reside there in the future may speak to his subjective expectation of privacy, but they fall short of establishing circumstances on which an objectively reasonable expectation of privacy could be based.”); *United States v. Angevine*, 281 F.3d 1130, 1134 n.1 (10th Cir. 2002) (“Because we conclude society is not prepared

Circuits.⁸⁵ The Ninth Circuit also applies Harlan's framework consistently⁸⁶ but sometimes drifts into the language of a "legitimate expectation" as shorthand for the two prongs.⁸⁷

Finally, while the First Circuit has sometimes used Harlan's test,⁸⁸ it does not always do so. In *United States v. Paradis*,⁸⁹ the court only used a reasonable expectation standard,⁹⁰ never referring to the two prongs. In *United States v. Dunning*,⁹¹ the court set up Harlan's framework when it stated that the "[defendant] contends that he had an expectation of privacy in a letter sent to a girlfriend with whom he had an intimate relationship and an understanding that the two would save their letters to each other, and that this expectation ought to be recognized as reasonable."⁹² However, the court dismissed the two-pronged approach and applied a "legitimate and reasonable

to recognize as reasonable an expectation of privacy in the seized University computer, we need not consider whether Professor Angevine himself had a subjective expectation of privacy.").

84. See *United States v. Segura-Baltazar*, 448 F.3d 1281, 1286–87 (11th Cir. 2006) (analyzing the subjective and objective expectations of privacy for garbage placed near the curb for the trash collector); *United States v. Miravalles*, 280 F.3d 1328, 1331–33 (11th Cir. 2002) (holding that there is neither a subjective nor objectively reasonable expectation to privacy in a large, high-rise apartment building, where the front door has an undependable lock).

85. See *United States v. Askew*, 529 F.3d 1119, 1127 (D.C. Cir. 2008) ("By zipping up his jacket, appellant unquestionably evidenced an intent to keep private whatever lay under it. The only question, then, is whether society is prepared to recognize such an expectation as reasonable."); *Stewart v. Evans*, 351 F.3d 1239, 1243–44 (D.C. Cir. 2003) (holding that even if defendant held a subjective expectation of privacy in documents transferred from her place of employment, it was not a reasonable one).

86. See *United States v. Forrester*, 512 F.3d 500, 509–11 (9th Cir. 2008) (using Harlan's framework to analyze the computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of Web sites visited, and the total amount of data transmitted to or from an account); *United States v. Diaz-Castaneda*, 494 F.3d 1146, 1151 (9th Cir. 2007) (holding that people have neither a subjective nor an objectively reasonable expectation of privacy in a license plate); *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) ("The government does not dispute that [he] had a subjective expectation of privacy in his computer and his dormitory room, and there is no doubt that [his] subjective expectation . . . was legitimate and objectively reasonable.").

87. See *United States v. Davis*, 332 F.3d 1163, 1167–68 (9th Cir. 2003) ("[W]e do not conclude[] that Davis had less of a legitimate expectation of privacy in his gym bag than one would have in a suitcase [or] a purse [B]y placing his gym bag under the bed, Davis 'manifested an expectation that the contents would remain free from public examination.'" (citations omitted)).

88. See *United States v. Rheault*, 561 F.3d 55, 59 (1st Cir. 2009) ("We are satisfied that Rheault's decision to place the gun and drugs inside the washing machine on the third-floor landing sufficiently evidences an intent to hide them, and thus demonstrates a subjective expectation of privacy. . . . [W]e next turn to the much closer question of whether Rheault's subjective expectation was reasonable."); *United States v. Samboy*, 433 F.3d 154, 161 (1st Cir. 2005) ("We find that Samboy failed to argue his subjective privacy interest in the third-floor apartment in the court below. Moreover, Samboy has not pointed to any evidence to show that his interest in the apartment was one society would recognize as reasonable.").

89. 351 F.3d 21 (1st Cir. 2003).

90. See *id.* at 27, 32 (discussing only whether the defendant had a reasonable expectation of privacy and omitting any discussion of a two-pronged test).

91. 312 F.3d 528 (1st Cir. 2002).

92. *Id.* at 530–31.

expectation” standard, citing the Supreme Court’s decision in *Rakas v. Illinois*.⁹³ This is a sign that the First Circuit is not as faithful to Harlan as its other decisions suggest; the *Rakas* Court cited Justice Stewart’s majority opinion in *Katz*—not Harlan’s concurrence—as support for a test that determines “whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place.”⁹⁴ The *Dunning* opinion is an outlier, as later First Circuit decisions applied Harlan’s framework.⁹⁵ Yet even in a circuit that is generally faithful to Harlan, there is a sign of a return to a simpler framework.

b. Relaxed Adherence to Harlan’s Test.—There are other courts of appeals that cite Harlan’s framework but then proceed with a derivative standard. We might refer to this as relaxed adherence. The Sixth Circuit, for example, explained:

In analyzing whether a subjective expectation of privacy is objectively reasonable, this court considers a number of factors: (1) whether the defendant was legitimately on the premises; (2) his proprietary or possessory interest in the place to be searched or the item to be seized; (3) whether he had the right to exclude others from the place in question; and (4) whether he had taken normal precautions to maintain his privacy.⁹⁶

The first and second factors, of course, are a throwback to the pre-*Katz* framework on what is a search under the Fourth Amendment.⁹⁷ The Sixth Circuit, in another opinion, identified an additional factor: “whether [the defendant] has exhibited a subjective expectation that the area would remain free from governmental intrusion.”⁹⁸ The Fifth and Eighth Circuits also used these additional factors to decide subjective and objectively reasonable expectations of privacy.⁹⁹ While the Fifth, Sixth, and Eighth Circuits may be faithful to Harlan’s framework by accepting his labels and packaging, their lists of factors function more like Stewart’s totality-of-the-circumstances test.

93. *Id.* at 531 (citing *Rakas v. Illinois*, 439 U.S. 128, 143 (1978)).

94. *Rakas*, 439 U.S. at 143.

95. See *United States v. Rheault*, 561 F.3d 55, 59 (1st Cir. 2009) (using the two-part test for the expectation of privacy question); *United States v. Samboy*, 433 F.3d 154, 161 (1st Cir. 2005) (holding that there is no expectation of privacy because the defendant failed to argue a subjective privacy interest and because there is no evidence that the interest is one that society would recognize as reasonable).

96. *United States v. Dillard*, 438 F.3d 675, 682 (6th Cir. 2006).

97. See *United States v. Katz*, 389 U.S. 347, 352–53 (1967) (eschewing past cases that had used trespass standards and property interests in determining the applicability of the Fourth Amendment).

98. *United States v. Waller*, 426 F.3d 838, 844 (6th Cir. 2005).

99. See *United States v. Finley*, 477 F.3d 250, 258–59 (5th Cir. 2007) (using the factors to determine whether the defendant had a privacy interest in a company-issued cell phone); *United States v. Mendoza*, 281 F.3d 712, 715 (8th Cir. 2002) (applying the factors in deducing whether Mendoza had a legitimate expectation of privacy in a common area entryway in a duplex); *United States v. Runyan*, 275 F.3d 449, 457 (5th Cir. 2001) (using the factors to determine whether the defendant had a reasonable expectation of privacy in items found at his ranch).

Other opinions in the Fourth, Sixth, and Eighth Circuits cite the two-pronged approach but then gloss over the subjective expectation of privacy to focus only on the reasonable expectation prong. In a case about aerial surveillance, the Eighth Circuit “assume[d] without deciding that [the defendant] had a subjective expectation of privacy and focus[ed] on whether such an expectation could be objectively reasonable.”¹⁰⁰ The Fourth and Sixth Circuits have also acknowledged Harlan’s framework without coming back to it.¹⁰¹

The Fourth and Eighth Circuits also have outliers. In *United States v. Stevenson*,¹⁰² the Fourth Circuit discussed the two prongs in detail with specific facts from the record.¹⁰³ The Eighth Circuit, in analyzing whether a tape recording was a search, reasoned that “[the defendant] acknowledged, near the end of the conversation, that his statements were being recorded, and that this was ‘fine’ with him. Under these circumstances, [the defendant] could not reasonably expect that the conversation was private, and there was no search within the meaning of the Fourth Amendment.”¹⁰⁴ Nevertheless, both decisions are flanked by others that put their respective circuits within a camp of relaxed adherence to Harlan.

2. *Departure from Harlan.*—The Third Circuit departed from Harlan’s two-pronged framework to use the “legitimate expectation of privacy” standard from *Rakas*. In *United States v. Perez*,¹⁰⁵ the Third Circuit cited *Rakas* for the notion that the Fourth Amendment protects against searches where persons have “a legitimate expectation of privacy in the invaded place.”¹⁰⁶ It further explained:

Under this rule, persons in another’s apartment for a short time for the business purpose of packaging cocaine had no legitimate expectation

100. *United States v. Boyster*, 436 F.3d 986, 992 (8th Cir. 2006); *see also* *United States v. Brown*, 408 F.3d 1049, 1051 (8th Cir. 2005) (“There was no evidence Brown had a reasonable expectation of privacy in Lewis’s residence, because he was not present during the search, did not live at the residence, and did not have a key to the residence.”); *United States v. Hill*, 393 F.3d 839, 841 (8th Cir. 2005) (“These cases recognize that regardless of one’s subjective expectation of privacy in a public restroom, society’s recognition of that expectation of privacy is limited by the physical design of the restroom, [its] location . . . , and the probability that one will be asked to surrender use of the restroom to others.”).

101. *See* *United States v. Gray*, 491 F.3d 138, 145–46 (4th Cir. 2007) (analyzing whether the defendant was a social or business guest in Gray’s apartment and the appropriate level of privacy based on societal expectations); *United States v. Ellison*, 462 F.3d 557, 560–62 (6th Cir. 2006) (examining the reasonable expectations of a vehicle’s license plate); *United States v. Breza*, 308 F.3d 430, 433–35 (4th Cir. 2002) (determining the reasonable privacy expectations with regard to aerial surveillance of the curtilage).

102. 396 F.3d 538 (4th Cir. 2005).

103. *See id.* at 546–47 (analyzing whether the defendant, having shown an intention not to return to his apartment, had a reasonable expectation of privacy after his arrest).

104. *Sherbrooke v. City of Pelican Rapids*, 513 F.3d 809, 815 (8th Cir. 2008).

105. 280 F.3d 318 (3d Cir. 2002).

106. *Id.* at 337 (quoting *Minnesota v. Carter*, 525 U.S. 83, 88 (1998)).

of privacy in that apartment. Thus any search which may have occurred did not violate their Fourth Amendment rights. Although overnight guests who are legitimately in a third-party's apartment may have a reasonable expectation of privacy, Appellants do not qualify.¹⁰⁷

However, the Third Circuit has shown some fidelity to Harlan's framework by applying factors used by the Fifth, Sixth, and Eighth Circuits.¹⁰⁸ Even so, the Third Circuit's emphasis on places and privacy in other cases leaves *Perez* as an example of a departure from the two-pronged approach.¹⁰⁹ The Third Circuit thus welcomes Stewart over Harlan.

In the other circuits, Stewart's approach would obviate a mechanical application of Harlan's first prong, freeing the analysis to apply as many factors as are helpful to the specific facts of the case. Trespass is no longer an important factor, but the duration and the intensity of governmental action still matters to people protected by the Fourth Amendment. A return to Stewart would recognize all this in simpler terms.

C. Shortcomings of the Legal Framework

We have time before the next attack to reach a better equilibrium on physical surveillance. Related to the subway scenario that started this Article, I considered three types of surveillance: cameras, goggles, and detectors.¹¹⁰ Since the thwarted Christmas bombing plot in 2009¹¹¹ and President Obama's call to install more see-through scanners in American airports,¹¹² the public has been reminded that surveillance is not just an academic topic. Of the three forms of surveillance in our scenario, goggles would seem to present the most problems under the current Fourth Amendment framework.

107. *Id.* (citation omitted).

108. See *Warner v. McCunney*, 259 F. App'x 476, 477 (3d Cir. 2008) (using four factors that are relevant to showing a legitimate expectation of privacy: whether the party had a possessory interest, whether it could exclude others from the place, whether it took precautions to maintain privacy, and whether it had a key to the premises); *United States v. Hartwell*, 436 F.3d 174, 177 n.4 (3d Cir. 2006) (citing to *Kyllo* for the two-pronged approach but not analyzing the search because the government conceded the point).

109. See *Miller v. Hassinger*, 173 F. App'x 948, 952 (3d Cir. 2006) (citing *Minnesota v. Carter*, 525 U.S. 83, 88 (1998)) (providing that to demonstrate a constitutional privacy interest, an individual must establish a reasonable expectation of privacy in the place searched); *United States v. Schofield*, 80 F. App'x 798, 802 (3d Cir. 2003) (noting that the defendant must have a reasonable expectation of privacy in the automobile to have standing to challenge the search).

110. See *supra* notes 18–26 and accompanying text.

111. See Mark Hosenball et al., *The Radicalization of Umar Farouk Abdulmutallab*, NEWSWEEK, Jan. 11, 2010, at 37, 37 (discussing Abdulmutallab's personal background and the steps he took in his failed attempt to ignite an explosive device on a plane on Christmas Day 2009).

112. See Associated Press, *Body Scanners at More Airports: Passengers Can Choose Metal Detectors, Paid Down Instead*, GRAND RAPIDS PRESS, Mar. 14, 2010, at J4 (noting that the Obama Administration set aside \$1 billion of the \$787 billion stimulus package for airport screening, \$25 million of which was for body scanners).

The cameras on the agents' helmets would be recording people in public places; plus, those recordings would not be broadcast on television or the Internet. When a citizen walks down the street, he accepts that other people may be watching him—in the same way that cameras may be recording him.¹¹³ So, even if the United States veered toward the British practice of CCTV, it would not present a constitutional problem under current law or under my proposed reappraisal of the Fourth Amendment.¹¹⁴ In reaching these conclusions, I assume that the cameras perform a general scan of the crowd without zooming in on a person unless there is a particularized suspicion.

Similarly, the radiation detectors are safe under current law. The detectors, to be sure, are not limited to surface readings of people's movements. Even so, in line with Justice Stevens, I doubt people expect privacy for the radiological emanations of their belongings.¹¹⁵ Such expectations would not be legitimate.¹¹⁶ An agent who detects radiation with the assistance of basic technology is not different for purposes of the law from an agent who detects the smell of alcohol or marijuana from a suspect on the street. Neither the detection nor the smelling involves a search.¹¹⁷

113. Cf. John Buntin, *Long Lens of the Law*, GOVERNING, May 2009, at 24, available at <http://www.governing.com/article/long-lens-law> (praising security cameras as “force multipliers” that would allow a single police officer at a monitor to perform the surveillance work of several officers in the field).

114. See *Kyllo v. United States*, 533 U.S. 27, 31–32 (2001) (explaining that although “‘at the very core’ of the Fourth Amendment ‘stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion,’” this has never “‘require[d] law enforcement officers to shield their eyes when passing by a home on public thoroughfares”” (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961); *California v. Ciraolo*, 476 U.S. 207, 213 (1986))); *Dow Chem. Co. v. United States*, 476 U.S. 227, 238–39 (1986) (holding that aerial photography of a vast industrial complex did not constitute a search for Fourth Amendment purposes because there was no reasonable expectation of privacy); *Katz v. United States*, 389 U.S. 347, 361 (1967) (noting that “objects, activities, or statements that [a person] exposes to the ‘plain view’ of outsiders are not ‘protected’ because no intention to keep them to himself has been exhibited”).

115. See *Kyllo*, 533 U.S. at 43–44 (2001) (Stevens, J., dissenting) (“Heat waves . . . enter the public domain A subjective expectation that they would remain private is not only implausible but also surely not ‘one that society is prepared to recognize as “reasonable.”’” (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring))).

116. See, e.g., *California v. Greenwood*, 486 U.S. 35, 39–40 (1987) (holding that even if petitioners may have subjectively expected the contents to remain private, there is no legitimate expectation of privacy in trash left for collection in an area accessible to the public because society has not recognized an objectively reasonable expectation of privacy in such items); *id.* at 41 (“[A]s we have held, the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public.”); *United States v. Jacobsen*, 466 U.S. 109, 122 (1984) (“The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities.”); *supra* text accompanying note 39.

117. Cf. *United States v. Place*, 462 U.S. 696, 707 (1983) (holding that the use of a drug dog to detect drugs does not constitute a search under Fourth Amendment case law because the procedure

People do not have a legitimate expectation in the emanations of things they carry with them or in the smells, sounds, or sights they emit from their bodies. The governmental action to detect these things is not usually intense or longstanding.¹¹⁸

The goggles, unlike the cameras and the radiation detectors, see through a person's clothes. People, guilty or innocent, suspicious or inconspicuous, will be naked to the agents' eyes. The agents may see who has a replaced hip, a steel implant in the skull, or a pacemaker. Many people want to keep these facts private. If the devices detect plastics in addition to metals, the privacy concerns are more obvious. Some women do not want the world to know whether the contours to their bodies have been shaped, not by nature, but by a surgeon's scalpel.

My goal, to repeat, is to show *Katz's* limitations in protecting American privacy. Perpetual surveillance occurs with some suspects today; its relevance does not depend on another attack. The scenario about a subway attack serves as a reminder that physical surveillance can easily become very intrusive. As a result, a basic totality-of-the-circumstances test, rather than Justice Harlan's two-part test, is more useful in reaching the common-sense conclusion that at some point, 24/7 surveillance becomes intrusive enough to constitute a search. A search by the government then requires probable cause, reasonable suspicion, or, if individual suspicion is not there, some special need.¹¹⁹ Since the courts have recognized that there is a point at which a canine sniff can become intrusive enough to be a search,¹²⁰ they should be more forthright in recognizing that physical surveillance can switch categories just as easily. To me, Stewart's test seems more flexible than Harlan's for factoring the duration and the intensity of governmental action into the constitutional equation.

is limited "both in the manner in which the information is obtained and in the content of the information revealed by the procedure").

118. See *infra* subpart IV(C).

119. See U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation . . ."); *Illinois v. Lidster*, 540 U.S. 419, 424 (2004) (upholding the constitutionality of "information stops" and reiterating that searches absent particularized individual suspicion may be constitutional under the Fourth Amendment if special law enforcement purposes—other than general law enforcement—exist); *United States v. Arvizu*, 534 U.S. 266, 273 (2002) (reaffirming that, in some instances, a standard less than probable cause—"reasonable suspicion"—can support the reasonableness of a search in accordance with the Fourth Amendment).

120. See *United States v. Kelly*, 302 F.3d 291, 293 n.1 (5th Cir. 2002) (holding that up-close canine sniffing offends reasonable expectations of privacy and is therefore a search under the Fourth Amendment but that such searches, if routine, are permissible under the border-search exception to the warrant requirement); *B.C. v. Plumas Unified Sch. Dist.*, 192 F.3d 1260, 1266 (9th Cir. 1999) (holding that canine sniffs of high school students are Fourth Amendment searches); *United States v. Thomas*, 757 F.2d 1359, 1367 (2d Cir. 1985) (holding that a canine sniff outside an apartment door for the purposes of detecting drugs is a Fourth Amendment search). *But see* *United States v. Reed*, 141 F.3d 644, 649 (6th Cir. 1998) (holding that a canine sniff is not a search within the meaning of the Fourth Amendment).

Justice Stewart's totality-of-the-circumstances test does not eliminate ambiguity. No test can. Those who lean toward bright lines might actually prefer the emphasis on trespass that characterized Fourth Amendment jurisprudence before *Katz*.¹²¹ They may challenge both Justice Harlan and Justice Stewart. An advantage of the trespass test is that it avoids murky inquiries about expectations of privacy. The trespass test does not purport to determine whether sight, sound, or smell is more intrusive. Instead, trespass is about simple touch.¹²² As long as government agents do not touch suspects, do not touch their things, and do not stand on their property, the agents should be fine under the Fourth Amendment. Even under the law before *Katz*, constant surveillance was acceptable as long as it followed these rules. The time has come for change.

IV. Breakdown of the Framework

I am certainly not the first to criticize the Court's test for expectations of privacy.¹²³ But I am probably the most explicit, since 9/11, to suggest Justice Stewart's test as the replacement.

121. See *Kyllo v. United States*, 533 U.S. 27, 31 (2001) ("The permissibility of ordinary visual surveillance of a home used to be clear because, well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass." (citing *Goldman v. United States*, 316 U.S. 129, 134–36 (1942); *Olmstead v. United States*, 277 U.S. 438, 464–66 (1928))); cf. *Silverman v. United States*, 365 U.S. 505, 510–12 (1961) (relying on whether an "actual intrusion into a constitutionally protected area" had occurred rather than whether there had been a technical trespass in determining whether a Fourth Amendment search had occurred).

122. See *Olmstead*, 277 U.S. at 465–66 (holding that the Fourth Amendment applies only to physical searches and not to searches "by hearing or sight").

123. See, e.g., Amsterdam, *supra* note 9, at 385 (arguing that *Katz* "offers neither a comprehensive test of fourth amendment coverage nor any positive principles by which questions of coverage can be resolved"); Laurence A. Benner, *Diminishing Expectations of Privacy in the Rehnquist Court*, 22 J. MARSHALL L. REV. 825, 852 (1989) ("[T]he outcome of the *Katz* mode of analysis has increasingly resulted in the total loss of Fourth Amendment protection."); Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Trades Image and Identity*, 82 TEXAS L. REV. 1349, 1363 (2004) (arguing that Fourth Amendment jurisprudence "needs rethinking if constitutional privacy protections are to work well in twenty-first century conditions"); Morgan Cloud, *The Fourth Amendment During the Lochner Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 616–17 (1996) ("[O]ver the past thirty years the *Katz* approach has degenerated into a standardless 'expectations' analysis that has failed to protect either privacy or property interests."); Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 28–29 (2002) ("After a third of a century, it is fair to conclude that *Katz* is a failure. . . ."); Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 724 (1988) (arguing that since *Katz*, "the Supreme Court has determined that individual expectations of government surveillance, even when guarded against, appears wholly irrelevant"); Roberto Iraola, *New Detection Technologies and the Fourth Amendment*, 47 S.D. L. REV. 8, 8–9 (2002) (arguing that the Court has struggled to keep up with technology and that "[i]n the last thirty years, a number of investigative techniques—all found to fall outside the ambit of Fourth Amendment protection—have enabled the government to obtain details about our lives"); John M. Junker, *The Structure of the Fourth Amendment: The Scope of the Protection*, 79 J. CRIM. L. & CRIMINOLOGY 1105, 1183 (1989) ("The doctrinal record during the twenty years since *Katz*

A. Academic Opinions and Problems

Many scholars criticize the *Katz* framework for not doing enough to protect people against government snooping. Of those that criticize, however, very few wade into the differences between Stewart and Harlan. Their proposals for replacements can be broken into several groups—although I am mindful of the irony of doing so in an Article that says not to lose sight of the totality of circumstances.

A large group pushes for a return to a pre-*Katz* understanding of the Fourth Amendment, similar to the ruling in *Olmstead v. United States*.¹²⁴ This would tie the definition of a search to the concepts of property.¹²⁵ They

reveals a Court hostile to privacy and, of greater concern, willing to ignore or subvert the constraints of language and structure in its quest for the favored result.”); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 554 (1990) (declaring that “in the two decades since *Katz* was decided, the Court has applied the standard to reduce rather than enhance fourth amendment protections . . . allow[ing] the government access to many intimate details about our lives without having to establish the reasonableness of its behavior”); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 826–27 (2004) (“Indeed, scholars consistently denounce the Court’s opinions interpreting *Katz* as ‘dead wrong,’ ‘off the mark,’ ‘misguided,’ and ‘inconsistent with the spirit of the fourth amendment.’” (citation omitted)); Tracy Maclin, *Katz, Kyllo, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 51 (2002) (arguing that “the privacy and security protected by the Fourth Amendment should not depend on innovations in technology”); Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through Kyllo’s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1411 (2002) (arguing that *Katz* and its progeny do not sufficiently protect privacy since “[m]embers of our society should be constitutionally entitled to expect that government will refrain from any spying on the home—technological or otherwise—unless it can demonstrate good cause for doing so” (emphasis omitted)); William J. Stuntz, *Privacy’s Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016, 1048 (1995) (arguing that “[i]f we could start over, perhaps privacy would not receive constitutional protection anywhere”); George C. Thomas III, *Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451, 1500 (2005) (“The ‘expectation of privacy’ notion is flawed to the core.”); James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 438 (2002) (asserting that *Kyllo* insufficiently protects privacy since “[o]fficial exploitation of a scientific or technological device should be considered a Fourth Amendment search”); Daniel B. Yeager, *Search, Seizure and the Positive Law: Expectations of Privacy Outside the Fourth Amendment*, 84 J. CRIM. L. & CRIMINOLOGY 249, 251 (1993) (“*Katz* has been a dismal failure . . .”).

124. 277 U.S. 438 (1928).

125. See Cloud, *The Fourth Amendment During the Lochner Era: Privacy, Property and Liberty in Constitutional Theory*, *supra* note 123, at 628 (arguing that the Fourth Amendment’s “ultimate purposes, rooted in the history of the Amendment, were to protect individual liberty, privacy, and property, and to preserve the capacity to enjoy all three in the quiet of one’s home or place of business”); Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, *supra* note 123, at 47–50 (arguing that the jurisprudence should “emphasize the notion that the technological equivalent of a physical trespass can trigger a Fourth Amendment violation” as well as “extend this notion to settings outside of the interior of the home. At the very least, this should include other property that has traditionally received Fourth Amendment protection, including the home’s curtilage, closed containers like luggage, and the interior private commercial buildings,” and that “[t]his amalgam of property law, trespass theory, and technology could readily be extended to other settings”); see also Blitz, *supra* note 123, at 1364. Blitz argues that, as opposed to *Katz*’s famous pronouncement,

say when the government intrudes on a citizen's property, be it with the aid of technology or by physical entry, it should be a search. Professor Cloud, for example, contends that the "linkage between property, privacy, and liberty was more effective than is [the *Katz* rule] at implementing the Amendment's purposes and was more consistent with its text and history."¹²⁶ These critics say *Katz* changed very little of the analysis, since judges simply fall back on the time-tested rules of property law.¹²⁷

A second group pushes for a return to a more original interpretation of the Fourth Amendment,¹²⁸ comparable to what Scalia suggests in *Kyllo*.¹²⁹ For them, *Katz* has diluted the Fourth Amendment to allow police powers beyond the founders' vision. As Professor Davies argues, the "authentic history shows that framing-era doctrine provided a much stronger notion of a 'right to be secure' in person and house than does modern doctrine."¹³⁰ The originalists would more directly align the definition of a search with persons, houses, papers, and effects.¹³¹

[C]ourts can often best protect privacy in public life by focusing on places rather than the people who act in them. Instead of protecting individual expectations of privacy directly, courts might best protect privacy in public life indirectly by identifying and protecting those features of our society, including those features of public space, that allow anonymity and other privacy-related interests to exist in sufficient measure.

Id. (emphasis omitted); see also Slobogin, *supra* note 123, at 1411 (arguing that our society should be constitutionally protected from "any spying on the home—technology or otherwise—unless it can demonstrate good cause for doing so" (emphasis omitted)).

126. Cloud, *The Fourth Amendment During the Lochner Era: Privacy, Property and Liberty in Constitutional Theory*, *supra* note 123, at 563.

127. See, e.g., Orin S. Kerr, *Technology, Privacy, and the Courts: A Reply to Colb and Swire*, 102 MICH. L. REV. 933, 934 (2004) ("Even when purporting to protect privacy, judges have proven reluctant to deviate from rules based on principles of property law.").

128. See Benner, *supra* note 123, at 830 ("[F]or the Framers, the heart of the Fourth Amendment lay in the requirement that *individualized* justification be established under oath, as a necessary predicate to governmental intrusion."); Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 724 (1999) ("The Framers aimed the Fourth Amendment precisely at banning Congress from authorizing use of general warrants; they did not mean to create any broad reasonableness standard for assessing warrantless searches and arrests."); Thomas, *supra* note 123, at 1458 (explaining his method of inquiry as understanding "the common law relevant to search and seizure and the political context in which the Fourth Amendment was proposed and debated" and with this in mind proposing "a series of modifications based on what I think the Framers would have said if they could have seen particular modern police methods.").

129. See *Kyllo v. United States*, 533 U.S. 27, 35 (2001) (arguing that defining the term "search" to include obtaining information about the interior of the home that the government could not otherwise get without physical intrusion would provide the level of protection against government that existed at the time of the adoption of the Fourth Amendment); *supra* notes 41–54 and accompanying text.

130. Davies, *supra* note 128, at 749.

131. See Thomas, *supra* note 123, at 1459 ("[T]he Court's attempt to expand the coverage of the Fourth Amendment by restating it as protecting privacy is a failure. We need to return to the plain meaning of 'persons, houses, papers, and effects' as those items would be understood by the Framers in the context of modern life.").

A third group shifts away from the Search and Seizure Clause to highlight the Warrant Clause¹³² or the role that Congress should play.¹³³ One scholar proposes a bright-line rule: “[A]ll government use of sophisticated visual equipment . . . should be subject to the warrant requirement.”¹³⁴ Others say Congress is better suited than the Courts to address privacy in the context of rapid technological developments. Thus, it is up to the Legislature to develop “more nuanced, balanced, and accurate privacy rules when technology is in flux.”¹³⁵

Finally, similar to my position, a few scholars lend some support to Justice Stewart’s majority opinion, while criticizing *Katz*’s progeny.¹³⁶ For them, *Katz* is salvageable. According to Professor Swire, “[c]ourts could engage in a more substantive review of expectations of privacy in specific factual settings, and find that more categories of government action violate that test.”¹³⁷ For Swire and others, the solution to search problems depends on a threshold question. Professor Benner suggests asking “whether Fourth Amendment protection existed as a threshold matter, and then by

132. See, e.g., Amsterdam, *supra* note 9, at 417 (“A paramount purpose of the fourth amendment is to prohibit arbitrary searches and seizures as well as unjustified searches and seizures. The warrant requirement was the framers’ chosen instrument to achieve both purposes, and it should continue to be applied to those ends. . . .”); Gutterman, *supra* note 123, at 732 (“We must bring technology under the umbrella of the procedural protections of the warrant clause.”); David E. Steinberg, *Making Sense of Sense-Enhanced Searches*, 74 MINN. L. REV. 563, 629 (1990) (asserting that “[n]owhere is an appropriate application of the warrant clause more essential to protect the security promised by the fourth amendment” than for sense-enhancing technologies).

133. See Amsterdam, *supra* note 9, at 380 (arguing that effective control over police practices depends upon, among other things, the creation of new regulatory devices subject to court oversight); Raymond Shih Ray Ku, *The Founders’ Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1375–76 (2002) (arguing that the Fourth Amendment should be interpreted to require legislative approval of any governmental use of new technologies to better protect privacy against these new innovations).

134. Gutterman, *supra* note 123, at 733.

135. Kerr, *supra* note 123, at 807–08. “Legislatures do not offer a panacea, but they do offer significant institutional advantages over courts.” *Id.* at 807.

136. See Gutterman, *supra* note 123, at 666 (“The damage had been done in his *Katz* concurrence. By basing *Katz* on a subjective expectation analysis and thereby a risk-assumption theory, Justice Harlan subjected each and every member of society to unimagined risks.”); Junker, *supra* note 123, at 1178 (“*Katz*’ weakness, however, is also its strength. It bends in both directions.”); Katz, *supra* note 123, at 560–63 (arguing that *Katz* “provided a framework for ensuring freedom by protecting personal security”); Scott E. Sundby, “*Everyman*’s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?”, 94 COLUM. L. REV. 1751, 1755–56 (1994) (arguing that *Katz* could be the framework for the future of trust in the government); Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 905 (2004) (arguing that with the development of new technology, *Katz* may be “dead for [its] core facts,” but that Fourth Amendment doctrine should continue to play a role in governing high-tech searches); James J. Tomkovicz, *Beyond Secrecy for Secrecy’s Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 737 (1985) (proposing an “instrumental approach to resolving fourth amendment threshold questions [that] will further [the] realization of the full potential of the *Katz* revolution”); Yeager, *supra* note 123, at 308 (arguing that though the test is flawed, “[w]hen the government is behaving lawfully, *Katz* acts as a backstop, as a second look at whether the positive law fairly reflects a given defendant’s expectations”).

137. Swire, *supra* note 136, at 923.

determining whether that protection had, nevertheless, been waived because it was reasonably foreseeable that the details actually observed by the police would have also been observed by members of the public.”¹³⁸ A search has occurred if this threshold test is answered in the positive.¹³⁹

B. *Common-Sense Answers*

Justice Harlan’s two-part test cuts out the common sense necessary to decide whether governmental action is a search. Lost between two layers of analysis are facts about the depth and duration of the intrusion. The Fourth Amendment is as much about places as it is people. When we put ourselves into public settings—a train station, the airport, a subway car, or the street—we know other people are observing us, but our expectation is for these observations to be brief and fleeting. Don’t stare at me and I won’t stare at you. We blend into the crowd. But if someone looks at us for too long, we become self-conscious. Our anonymity has disappeared, and the exchange with the observer might become violent, romantic, or something in between. The tipping point from anonymity to being in the imaginary crosshairs is not precise. It could take five seconds or ten seconds, but we know when our space has been violated. These are obvious points, but the jurisprudence of searches tends to ignore them. Today the prevalence of CCTV in the private sector, rather than decrease a citizen’s constitutional protections, should mean that the government’s addition of visual surveillance more readily tips the balance toward a search under the Fourth Amendment.

Moreover, despite all the talk about expectations of privacy, it is not clear whether Justice Harlan had in mind a person’s expectations about all possible intrusions (public and private) or just public intrusions. Depending on the facts, a person may have a different assessment of whether a cop or a private citizen is lurking about, and society’s decision about what is reasonable may also be affected.

In practice, the cases do not often turn on the first part of the Harlan test. Many cases in state and federal courts are decided without reported opinions.¹⁴⁰ The defendant who files a motion to suppress will allege that he expected to be free of the government conduct. The government can try to show facts that rebut the defendant’s allegation or, conceding the first part of Harlan’s test, it can move on to the second part. Further, Harlan’s test has other problems. A pure application of Harlan’s test would allow the government to lessen and perhaps eliminate expectations by a ratcheting of more

138. Benner, *supra* note 123, at 871–72.

139. *See id.* at 872 n.214 (“By liberally construing the language of the Amendment to effect its purpose in protecting privacy as mandated by *Boyd v. United States*, 116 U.S. 616, 635 (1886), much of the need for a Katzian analysis would disappear.”).

140. *E.g.*, *United States v. Davis*, No. 09-30047, 2010 WL 610646 (C.D. Ill. Feb. 11, 2010); *Young v. Commonwealth*, No. 2007-CA-002049-MR, 2010 WL 323120 (Ky. Ct. App. Jan. 29, 2010); *State v. Hoskinson*, No. 2 CA-CR 2008-0408, 2009 WL 3068990 (Ariz. Ct. App. Sept. 25, 2009).

intrusive activity. Justice Harlan himself eventually recognized this problem. In dissent in *United States v. White*, he noted that the purpose of the Fourth Amendment is “to form and project, as well as mirror and reflect.”¹⁴¹ Subjectivity was balanced by some court-imposed objectivity.

More commonly in Fourth Amendment cases, the government concedes that the defendant had a subjective expectation of privacy and then moves on to contest whether the second part of the test has been met.¹⁴² These concessions collapse the test into one line of inquiry on whether the expectations are reasonable. Thus, the second prong becomes a means for applying Stewart’s test, whether or not the parties and the judges acknowledge it. Although Justice Stewart and Justice Harlan both agreed that the Fourth Amendment “protects people, not places,”¹⁴³ the Supreme Court and the lower courts have considered the location of the government activity as a factor in determining “reasonable” expectations.¹⁴⁴ Justice Scalia’s opinion in *Kyllo*, as one example, cannot be fully appreciated without remembering that the thermal imaging was directed at a home, arguably the most protected place.¹⁴⁵

Yet both *Olmstead* and Harlan’s *Katz* concurrence are out of date for the modern world. As seen in the debate between Justice Scalia and Justice Stevens in *Kyllo*, the distinctions between touch, sight, sound, and smell can break down.¹⁴⁶ Courts continue to guess at our expectations of privacy. Often people are too private to speak about their privacy. By taking you to the toilet, I discuss important things that squeamish judges and other people may avoid in their opinions and their conversations.

C. Harlan’s Test Exposed

Imagine you have entered a public bathroom at the airport in Minneapolis–Saint Paul. You pick the far stall because it is a bit larger than the others and because the stall next to it is empty. You clean the toilet lid before you sit down. You grab a piece of leftover newspaper from the floor, pull your pants down, and sit down to relieve yourself. Later you find out an

141. 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

142. See, e.g., *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (noting that the Government did not dispute that the defendant had a subjective expectation of privacy, then holding that his expectation was reasonable); *United States v. Goldsmith*, 432 F. Supp. 2d 161, 169 (D. Mass. 2006) (noting that even though the reasonableness of the defendant’s expectation of privacy was at issue, the Government did not dispute his subjective expectation of privacy).

143. *Katz v. United States*, 389 U.S. 347, 351 (1967).

144. See *supra* subpart III(B); see also, e.g., *Kyllo v. United States*, 533 U.S. 27, 37 (2001) (noting that in the home “all details are intimate details”); *United States v. King*, 509 F.3d 1338, 1342 (11th Cir. 2007) (concluding that there is no reasonable expectation for privacy from a government search conducted through a computer connection to a common network drive); *United States v. Villegas*, 495 F.3d 761, 767 (7th Cir. 2007) (holding that there is no reasonable expectation for privacy in a common hallway of a duplex).

145. *Kyllo*, 533 U.S. at 29.

146. See *supra* text accompanying notes 41–58.

airport policeman was “monitoring” you in one of three ways.¹⁴⁷ First, a deaf agent with no sense of smell could have been above you, wedged in the ceiling. He peered down at you through a small hole. He only saw you in the middle of your business, not watching your preparations or your use of toilet paper after you flushed. He did not see your genitalia, only the sight of you reading with your pants down. Second, a blind and deaf agent could have been standing on the toilet seat in the stall next to you. He only smelled what you were doing. Third, a blind agent with no sense of smell could have been standing on the next toilet seat. He only heard what you were doing. Luckily for you, you get to pick which possibility is true.

Does it make sense to talk about different expectations of privacy for these three scenarios? Can we predict what possibility you and others will find the least invasive? The most? Have we in society really determined which expectations of privacy in the toilet stall we find reasonable? Have empirical studies gone that far? And, if so, are they reliable?

The *Olmstead* test would find these intrusions not to be a search.¹⁴⁸ You were in a public place, and the agent did not trespass on your constitutionally protected space. Both the Stewart test and the Harlan test would struggle to determine whether these intrusions were searches—assuming the agent gathered information of your illegal activity from the intrusion, you were arrested, and you contested the agent’s activity in a motion to suppress. The Harlan test, however, pretends to be more objective than it is. This Article, choosing Stewart over Harlan, strives to end those pretensions once and for all. Stewart’s totality-of-the-circumstances test makes more sense and is a

147. The monitoring of public bathrooms is not always hypothetical. Courts have held that whether bathroom surveillance is a search can depend on the location of the officer and the design of the stall. See *Kroehler v. Scott*, 391 F. Supp. 1114, 1118 n.4 (E.D. Pa. 1975) (finding that the expectation of privacy is controlled by the nature of the activity rather than the physical characteristics of the stall, or the even length of time in the bathroom); *Kirsch v. State*, 271 A.2d 770, 772 (Md. Ct. Spec. App. 1970) (holding that an officer unlocking and opening a bathroom door at the clerk’s request after three men had occupied it for thirty minutes did not constitute a search). Compare *Brown v. State*, 238 A.2d 147, 150 (Md. Ct. Spec. App. 1968) (holding that an officer sticking his head over a stall partition performed a search), and *State v. Bryant*, 177 N.W.2d 800, 804 (Minn. 1970) (holding that an officer surveying a stall through an overhead vent performed a search because the stall was completely secluded from outside view and the doors and stall assured the occupants of their privacy), with *Moore v. State*, 355 So. 2d 1219, 1221 (Fla. Dist. Ct. App. 1978) (holding that a police officer looking through a one-half inch crack in the bathroom stall door is not a search), and *Buchanan v. State*, 471 S.W.2d 401, 404 (Tex. Crim. App. 1971) (holding that police surveillance from a concealed position above a bathroom stall with no door was not a search because defendant had no reasonable expectation of privacy). Notoriously, bathroom surveillance resulted in the arrest of U.S. Senator Larry Craig in the men’s bathroom at Minneapolis–St. Paul International Airport on suspicion of lewd conduct in June 2007. *Senator, Arrested at Airport, Pleads Guilty*, N.Y. TIMES, Aug. 28, 2007, at A19. Police were cracking down after several complaints of sexual activity in the airport’s main men’s room. An officer stationed in a stall arrested Sen. Craig after he made signals that indicated he “[wished] to engage in lewd conduct.” Report from Sgt. Dave Karsnia, Minneapolis Airport Police Dept. (June 26, 2007), available at http://media.washingtonpost.com/wp-srv/politics/ssi/craig_police_report_082807.pdf.

148. See *supra* notes 124–27 and accompanying text.

more realistic summary of how courts and commentators struggle to balance individual and governmental interests.

V. Conclusion

You may not worry about the prospect of an extensive Government Toilet Surveillance Program. But you should worry about government intrusions that will come after the next attack. We are all reasonable in expecting a rational framework for determining whether a government surveillance program that includes cameras, goggles, and radiation detectors will constitute a search at some point. Justice Stewart's totality-of-the-circumstances test is better than Justice Harlan's two-part test in distinguishing brief periods of physical surveillance from constant surveillance that lasts days, weeks, months, or years. And Justice Stewart's test is much better for analyzing situations when various methods of surveillance are all combined.

Terrorism Trials and the Article III Courts After *Abu Ali*

Stephen I. Vladeck*

To say that it is difficult to divorce the debate over the suitability of trying terrorism suspects in the Article III courts from the politics of the moment would be an epic understatement. Especially in light of the Obama Administration's decisions to (1) try the "9/11 defendants" in the civilian courts¹ and (2) subject Umar Farouk Abdulmutallab to civilian—rather than military—jurisdiction,² recent months have witnessed a renewed barrage of objections to subjecting such extraordinary cases to the ordinary processes of our criminal justice system. These critiques have included claims that such trials make the city in which they occur a target for future attacks; that they provide the defendants with a platform from which to spew anti-American propaganda; that they risk publicly revealing information about intelligence sources and methods; that they are enormously costly both with regard to the security measures they require and the judicial resources they consume; and, most substantively, that they put pressure on the courts to sanction exceptional departures from procedural or evidentiary norms that will eventually become settled as the rule—what we might characterize as either a "distortion effect" or a "seepage problem."³

* Professor of Law, American University Washington College of Law. My thanks to Bobby Chesney for inviting me to participate in the symposium for which this essay was prepared; to the staff of the Texas Law Review for their coordination, editing, and patience; and to Heather Sokolower for exceptional research assistance.

1. See, e.g., Peter Finn & Carrie Johnson, *Alleged Sept. 11 Planner Will Be Tried in New York*, WASH. POST, Nov. 14, 2009, at A1 (reporting that the "self-proclaimed mastermind of the Sept. 11, 2001[] attacks, and four co-conspirators will be tried in Manhattan federal courthouse"). But see Jane Mayer, *The Trial: Eric Holder and the Battle over Khalid Sheikh Mohammed*, NEW YORKER, Feb. 15 & 22, 2010, at 52 (noting the ongoing controversy over whether the 9/11 defendants should be tried in civilian court, and the Obama Administration's reconsideration of its original decision).

2. See, e.g., Letter from Eric Holder, U.S. Attorney General, to Mitch McConnell, U.S. Senator (Feb. 3, 2010), available at <http://www.justice.gov/cjs/docs/ag-letter-2-3-10.pdf> (explaining the reasons behind the Attorney General's decision to charge Umar Farouk Abdulmutallab in federal court).

3. See Michael B. Mukasey, Op-Ed., *Jose Padilla Makes Bad Law*, WALL ST. J., Aug. 22, 2007, at A15 (voicing concerns about revealing methods and sources of intelligence, the strain on security and financial resources, and the legal distortions that may occur); Michael B. Mukasey, *Where the U.S. Went Wrong on Abdulmutallab*, WASH. POST, Feb. 12, 2010, at A27 (same); Vincent J. Vitkowsky, *Try Mohammed at Guantanamo*, HUFFINGTON POST, Mar. 19, 2010, http://www.huffingtonpost.com/vincent-j-vitkowsky/try-mohammed-at-guantanam_b_505850.html (arguing that holding 9/11 trials in the United States would provide a forum for defendants to voice anti-American propaganda and make the cities in which the trials are held prone to future terrorist attacks); John Yoo, Op-Ed., *The KSM Trial Will be an Intelligence Bonanza for al Qaeda*,

These arguments are not new.⁴ Nevertheless, they do raise fundamental questions about whether the civilian courts are able to effectively function in certain high-profile terrorism cases and to balance the rights of the defendants with the very real practical, logistical, and substantive difficulties that such prosecutions tend to raise. Moreover, the answers may themselves have much to say about the normative desirability of possible alternatives, especially trials by military commission—at least in those cases in which such courts *could* legally exercise jurisdiction.⁵

A series of reports by different institutions and organizations, including the ABA's Standing Committee on Law and National Security,⁶ the Center on Law and Security at NYU School of Law,⁷ and Human Rights First,⁸

WSJ.COM, Nov. 15, 2009, <http://online.wsj.com/article/SB10001424052748704431804574537370665832850.html> (arguing that any civilian trials of the 9/11 defendants will likely reveal intelligence sources and methods to al Qaeda). For a broader and more general discussion of the seepage problem, see LAURA K. DONOHUE, *THE COST OF COUNTERTERRORISM: POWER, POLITICS, AND LIBERTY* (2008) (examining how procedural exceptions adopted to deal with extreme cases in the British legal system inexorably became hard-wired into the rules).

4. Several years ago, when proposals for "national security courts" were in vogue, *see, e.g.*, GLENN SULMASY, *THE NATIONAL SECURITY COURT SYSTEM: A NATURAL EVOLUTION OF JUSTICE IN AN AGE OF TERROR* 157–93 (2009) (arguing for the establishment of a national security court system), similar arguments were made about the inability of the Article III courts to handle terrorism prosecutions effectively. I am on record as being a vocal critic of such proposals, for reasons I have articulated elsewhere. *See, e.g.*, Stephen I. Vladeck, *The Case Against National Security Courts*, 45 WILLAMETTE L. REV. 505, 523–25 (2009).

5. For a brief survey of some of the military commissions' potential jurisdictional issues, see generally Stephen I. Vladeck, *On Jurisdictional Elephants and Kangaroo Courts*, 103 NW. U. L. REV. COLLOQUY 172 (2008), <http://www.law.northwestern.edu/journals/lawreview/Colloquy/2008/40>. The Congressional Research Service has provided a useful comparison of the procedural rights available to defendants under the current military commission system, as compared to trial in civilian criminal court. JENNIFER K. ELSEA, CONG. RESEARCH SERV., *COMPARISON OF RIGHTS IN MILITARY COMMISSION TRIALS AND TRIALS IN FEDERAL CRIMINAL COURT* (2010), available at <http://www.fas.org/sgp/crs/natsec/R40932.pdf>; *see also* Kenneth Jost, *Prosecuting Terrorists: Should Suspected Terrorists Be Given Civil or Military Trials?*, 20 CQ RESEARCHER 217 (2010) (discussing the issues surrounding whether suspected terrorists should be tried by civil or military courts). For a more in-depth analysis of the potential constitutional limits on the jurisdiction of military commissions, see Stephen I. Vladeck, *The Laws of War as a Constitutional Limit on Military Jurisdiction*, 4 J. NAT'L SEC. L. & POL'Y (forthcoming 2010).

6. ASHELY INDERFURTH & WAYNE MASSEY, A.B.A. STANDING COMM. ON LAW & NAT'L SEC. ET AL., *TRYING TERRORISTS IN ARTICLE III COURTS: CHALLENGES AND LESSONS LEARNED* (2009), http://www.abanet.org/natsecurity/trying_terrorists_artIII_report_final.pdf; STEPHEN I. VLADECK, A.B.A. STANDING COMM. ON LAW & NAT'L SEC. ET AL., *DUE PROCESS AND TERRORISM* (2007), http://www.abanet.org/natsecurity/publications/due_process_and_aba_stcolns_nsf_mtf.pdf.

7. CTR. ON LAW & SEC., N.Y.U. SCH. OF LAW, *TERRORIST TRIAL REPORT CARD* (2010), <http://www.lawandsecurity.org/publications/TTRCFinalJan14.pdf> [hereinafter *TERRORIST TRIAL REPORT CARD*].

8. RICHARD B. ZABEL & JAMES J. BENJAMIN, JR., *HUMAN RIGHTS FIRST, IN PURSUIT OF JUSTICE: PROSECUTING TERRORISM CASES IN THE FEDERAL COURTS* (2009), available at <http://www.humanrightsfirst.org/pdf/090723-LS-in-pursuit-justice-09-update.pdf>; RICHARD B. ZABEL & JAMES J. BENJAMIN, JR., *HUMAN RIGHTS FIRST, IN PURSUIT OF JUSTICE: PROSECUTING TERRORISM CASES IN THE FEDERAL COURTS* (2008), available at <http://www.humanrightsfirst.info/pdf/080521-USLS-pursuit-justice.pdf>.

among others, have offered various quantitative and qualitative assessments of the work of the Article III courts in post-9/11 terrorism cases. Although the reports differ in material ways, they all reflect to some degree a sentiment expressed quite pointedly in the *Terrorist Trial Report Card* prepared by the NYU School of Law's Center on Law and Security, i.e., that "the overwhelming evidence suggests that the structures and procedures, as well as the substantive precedents, provide a strong and effective system of justice for alleged crimes of terrorism."⁹

These reports, though, have all looked at the challenges faced by the Article III courts at the macro level, gathering copious data on the hundreds of terrorism or terrorism-related prosecutions to have taken place since September 11 and drawing conclusions from the aggregated results.¹⁰ In the Article that follows, I attempt a different approach, focusing on the specific procedural and evidentiary issues confronted in one of the more legally significant of the post-9/11 criminal prosecutions completed as of this Article—the trial of Ahmed Omar Abu Ali.¹¹

Abu Ali's case is thought-provoking, if not fascinating, on any number of levels,¹² including the strange (and potentially troubling) circumstances in which it began;¹³ the uniqueness of the charges against him—which included conspiracy to assassinate the President in addition to a host of more conven-

9. TERRORIST TRIAL REPORT CARD, *supra* note 7, at iv.

10. One recent exception is a fantastic report put together by the Federal Judicial Center, documenting the particular case-management challenges that individual trial courts have confronted in post-9/11 terrorism cases. ROBERT TIMOTHY REAGAN, FED. JUD. CTR., NATIONAL SECURITY CASE STUDIES: SPECIAL CASE-MANAGEMENT CHALLENGES (2010), available at [http://www.fjc.gov/public/pdf.nsf/lookup/ts100222.pdf/\\$file/ts100222.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/ts100222.pdf/$file/ts100222.pdf).

11. *United States v. Abu Ali*, 528 F.3d 210 (4th Cir. 2008). Perhaps the best indicator of the significance of *Abu Ali* is the fact that the members of the three-judge Fourth Circuit panel that heard the appeal issued a joint, signed opinion affirming Abu Ali's conviction. *Id.* at 220–21; see also John Ashcroft, *Reflections on Events and Changes at the Department of Justice*, 32 HARV. J.L. & PUB. POL'Y 813, 828–29 (2009) (referring to *Abu Ali* as one of the Bush Administration's successful terrorist prosecutions). For a cursory summary of the case and the unique issues it raised, see REAGAN, *supra* note 10, at 125–31.

12. There have been other (perhaps *more* significant) terrorism prosecutions since September 11, most notably the prosecution of the alleged "twentieth hijacker," Zacarias Moussaoui. At least as relates to the current project, my own view is that *Abu Ali* is a better case study, if for no other reason than because it, unlike *Moussaoui*, went to trial. See, e.g., *United States v. Moussaoui*, 591 F.3d 263, 266 (4th Cir. 2010) (noting Moussaoui pleaded guilty). *Abu Ali* is also a more compelling choice—at least for the moment—than the prosecution of Jose Padilla, whose appeal of his conviction remains pending before the Eleventh Circuit as of this writing. See *United States v. Hassoun*, No. 04-60001 ACR, 2007 WL 4180844 (S.D. Fla. Nov. 20, 2007) (denying Padilla and his co-defendants' post-trial motion for judgment of acquittal); *United States v. Hassoun*, No. 04-60001 ACR, 2007 WL 4180847 (S.D. Fla. Nov. 20, 2007) (denying the defendants' motion for a new trial).

13. See *Abu Ali v. Ashcroft*, 350 F. Supp. 2d 28, 31 (D.D.C. 2004) (denying the Government's motion to dismiss Abu Ali's habeas petition, which alleged that he was being held—and tortured—in Saudi Arabia at the behest of U.S. government officers), *dismissed as moot*, 387 F. Supp. 2d 16 (D.D.C. 2005).

tional post-9/11 terrorism counts;¹⁴ the procedural innovations adopted by the district court to allow Saudi intelligence officials to provide remote deposition testimony outside the presence of the defendant (and notwithstanding Rule 15 of the Federal Rules of Criminal Procedure);¹⁵ the thorny question of whether *Miranda*¹⁶ applied to certain statements that Abu Ali gave while in Saudi custody, albeit with American interrogators in the room—the only substantive issue at trial to divide the three-judge panel of the Fourth Circuit on appeal;¹⁷ and the clear violation of the Sixth Amendment’s Confrontation Clause at trial, which the Fourth Circuit held to constitute harmless error¹⁸ (a ruling that itself formed the basis for an unsuccessful petition for a writ of certiorari to the Supreme Court).¹⁹

In short, *Abu Ali* is a microcosm of both the unique difficulties these cases present and the ways in which such issues have generally been resolved by federal trial judges exercising creativity and flexibility. Moreover (and more specifically relevant to this Symposium), *Abu Ali* provides particular proof of the extent to which advancements in courtroom technology may well mitigate at least some of the practical obstacles that courts face in transnational terrorism cases. Finally, whatever difficulties *Abu Ali* may have presented for the civilian criminal justice system, it is difficult to see how the same difficulties wouldn’t also be present had Abu Ali been tried in a military commission. The claimed errors at trial that were analyzed by the Fourth Circuit were all constitutionally grounded, and there is little in the way of precedent for the proposition that either the Fifth Amendment’s privilege against self-incrimination or the Sixth Amendment’s right to confrontation have less force before a military tribunal—especially where the defendant is a U.S. citizen.²⁰

14. See Indictment at 13, *United States v. Abu Ali*, Crim. No. 1:05CR53 (E.D. Va. Feb. 3, 2005), available at <http://news.findlaw.com/hdocs/docs/terrorism/abuali20305ind.pdf> (listing the conspiracy to assassinate charge under count four, “Providing Material Support and Resources to Terrorists”).

15. See Barry M. Sabin et al., *Proposed Changes to Federal Rule of Criminal Procedure 15: Limitations, Technological Advances, and National Security Cases*, in TERRORIST TRIAL REPORT CARD, *supra* note 7, at 34, 34 & n.2 (citing *Abu Ali* as an example where foreign depositions were utilized).

16. *Miranda v. Arizona*, 384 U.S. 436 (1966).

17. See *United States v. Abu Ali*, 528 F.3d 210, 229–30 & nn.5–6 (4th Cir. 2008) (presenting the competing views for the three-judge panel on the issue of whether the American interrogators’ presence constituted a joint venture). Judge Motz’s published dissent focused entirely on her disagreement with the majority over Abu Ali’s sentencing, see *id.* at 269–82 (Motz, J., dissenting), an issue beyond the scope of this Article.

18. *Id.* at 256–57.

19. See *Petition for Writ of Certiorari at i, Abu Ali v. United States*, 129 S. Ct. 1312 (2009) (No. 08-464) (framing as the sole question presented whether “a Sixth Amendment violation involving the presentation of evidence to the jury in a criminal prosecution, which evidence the defendant is denied the right to see, [can] ever constitute harmless error”).

20. Cf. *United States v. Blazier*, 68 M.J. 439, 441–42 (C.A.A.F. 2010) (applying standard Sixth Amendment Confrontation Clause analysis to review a court-martial); *United States v. Chatfield*, 67 M.J. 432, 439–40 (C.A.A.F. 2009) (applying standard Fifth Amendment self-incrimination analysis

To be sure, like this Article's conclusions, its aim is modest. There are a host of reasons why it would be wrong to draw sweeping lessons from the story of one particular case, no matter how significant that one case may be. In addition, even an assessment of *just* the *Abu Ali* litigation is lacking for any appreciation of the myriad problems that Government or defense counsel likely encountered behind the scenes; the story told here is one reconstructed entirely from the public record, a record that could also be read with a far more skeptical eye.²¹ Nevertheless, my hope is that a candid discussion of the *Abu Ali* litigation—including its triumphs and its shortcomings—will add meaningful substantive content to a conversation that, for the moment, seems awash in unsubstantiated (and largely partisan) rhetoric.

To that end, Part I of the Article provides a detailed summary of the litigation, from the habeas proceedings initiated while Abu Ali was still in Saudi custody, to the various pre-trial rulings by Judge Gerald Bruce Lee of the U.S. District Court for the Eastern District of Virginia, to the trial itself, to Abu Ali's subsequent appeal to the Fourth Circuit, and finally to his (unsuccessful) petition for certiorari.

Part II turns to a brief analysis of the three most prominent issues that arose out of Abu Ali's trial—the improvised deposition procedures employed by the district court, the introduction of un-Mirandized statements made while Abu Ali was still in Saudi custody, and the Confrontation Clause error that was ultimately adjudged to be harmless. As Part II suggests, the first issue shows how the judicious use of courtroom technology can better balance the rights of the defendant with the security and foreign policy concerns of the government in terrorism prosecutions, the second issue highlights the difficulties courts face in applying precedents forged in traditional law enforcement to multinational counterterrorism investigations, and the third issue reinforces the extent to which, even when courts and policy makers *have* attempted to take all relevant concerns into account, honest mistakes will still be made. As harmless error doctrine recognizes, though, our criminal justice system commits any number of decisions to the sound discretion of trial judges, and relief therefore turns not on the existence of error, but on the extent to which the errors prejudice the overall integrity of the trial

to review a court-martial). It is possible, of course, that constitutional protections enjoyed by court-martial defendants may not be available to non-citizens tried by a military commission, but that is an open question, at the very least (and one that would not be implicated in Abu Ali's case). Moreover, at least one circuit has expressly held that the Fifth Amendment's right against self-incrimination requires the equivalent of *Miranda* warnings even for non-citizens detained outside the territorial United States. See *In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 177, 203–04 (2d Cir. 2008).

21. See, e.g., Wadie E. Said, *Coercing Voluntariness*, 85 IND. L.J. 1, 25–34 (2010) (summarizing—and criticizing—the various discussions of voluntariness by the district court and Fourth Circuit in *Abu Ali*); see also Jenny-Brooke Condon, *Extraterritorial Interrogation: The Porous Border Between Torture and U.S. Criminal Trials*, 60 RUTGERS L. REV. 647 (2008) (using *Abu Ali* to argue for clearer standards for the admissibility of statements obtained via foreign interrogations).

proceedings.²² And while some may believe that harmless error doctrine has become *too* ubiquitous as a safety valve in contemporary criminal prosecutions, that is hardly a charge that is specific to terrorism trials. In short, *Abu Ali* is a mixed bag, and we would do well to appreciate its positive lessons, to reflect upon its negative lessons, and to accept, perhaps with a grain of salt, the Fourth Circuit's suggestion that *Abu Ali* is a reminder of a familiar principle—"while 'the Constitution entitles a criminal defendant to a fair trial,' it does not guarantee 'a perfect one.'"²³

I. The *Abu Ali* Litigation

A. Background, Arrest, and the Habeas Petition

Ahmed Omar Abu Ali is a U.S. citizen who was born in Texas and raised in the Virginia suburbs of Washington, D.C.²⁴ In September 2002, at the age of 21, he left home to study at the Islamic University in Medina, Saudi Arabia.²⁵ Nine months later, he was arrested by officers of the Mabahith—the counterterrorism security forces of the Saudi Ministry of the Interior—who had come to believe that he was affiliated with the terrorist cell (al-Faq'asi) responsible for the May 12, 2003 suicide attacks in Riyadh that had killed thirty-nine people, including nine Americans, and that he was involved in planning for future al-Faq'asi and al Qaeda attacks on U.S. soil.²⁶ As subsequent testimony would reveal, a suspect detained in the Mabahith's investigation into the May 12 attacks had identified a photograph of Abu Ali from a Medina University student photo book and informed the Mabahith that the man he identified was a cell member known as "Reda," an American or European citizen of Arabian background.²⁷ Investigators subsequently identified "Reda" as Abu Ali and orchestrated his capture.²⁸

22. See *Neder v. United States*, 527 U.S. 1, 18–19 (1999) (noting the role played by harmless error doctrine). See generally ROGER J. TRAYNOR, *THE RIDDLE OF HARMLESS ERROR* 50 (1970) ("Like all too easy affirmance, all too ready reversal is also inimical to the judicial process. Again, nothing is gained from such an extreme, and much is lost. Reversal for error, regardless of its effect on the judgment, encourages litigants to abuse the judicial process and bestirs the public to ridicule it.").

23. *Abu Ali*, 528 F.3d at 256 (quoting *Delaware v. Van Arsdall*, 475 U.S. 673, 681 (1986)).

24. The facts are variously taken from three sources: the district court's decision denying Abu Ali's motion to suppress and motion to dismiss the criminal indictment, *United States v. Abu Ali*, 395 F. Supp. 2d 338, 343–48 (E.D. Va. 2005); the Fourth Circuit's decision affirming Abu Ali's conviction, *Abu Ali*, 528 F.3d at 221–26; and the D.C. district court's decision denying the Government's motion to dismiss Abu Ali's habeas petition, *Abu Ali v. Ashcroft*, 350 F. Supp. 2d 28, 31–36 (D.D.C. 2004). It bears emphasizing that, at least in the last opinion, the facts alleged in Abu Ali's habeas petition were taken as true in order to resolve the Government's motion to dismiss. *Abu Ali*, 350 F. Supp. 2d at 31 n.1.

25. *Abu Ali*, 528 F.3d at 221.

26. *Abu Ali*, 395 F. Supp. 2d at 343–44.

27. *Id.* at 344.

28. *Id.* at 344–45.

After Abu Ali was arrested by the Mabahith, he was held at first in Medina, and his dorm room was searched by Saudi law enforcement officials.²⁹ The warden of the facility where he was detained “adamantly denied that Mr. Abu Ali was tortured, beaten, deprived of sleep, or questioned in Medina.”³⁰ Abu Ali, on the other hand, alleged that he was not fed on his first day in custody in Medina and that Saudi officials hit him, “slapp[ed] him, punched him in the stomach, and pulled his beard, ears, and hair” on the night of his arrest.³¹ Abu Ali further testified that the beatings continued on his second day in custody but ceased after he agreed to cooperate with the investigation.³² Contrary to testimony given by Saudi officials, who claimed that he was not interrogated in Medina, Abu Ali maintained that he was interrogated on both the second and third day during which he was held in custody at the facility in Medina.³³

Several days after his arrest, Abu Ali was transported to a prison in Riyadh, where he made a number of incriminating statements regarding his participation in past and future terrorist plots.³⁴ His principal interrogators in Riyadh—the brigadier general and the captain of the Mabahith who ran the prison—would later stringently deny that “they directed, participated in, or were aware of any government official torturing Mr. Abu Ali or engaging in any such behavior.”³⁵ The brigadier general would testify that their interrogations began in the evening and continued into the early morning hours but insisted that this was customary in Saudi Arabia because of the country’s very hot weather and that the timing of the interrogation was not an attempt to deprive Abu Ali of sleep.³⁶ He also testified that Abu Ali was granted “breaks, access to food, water, a bathroom, and refreshments during breaks in questioning.”³⁷ Abu Ali himself conceded that “Riyadh wasn’t as bad as Medina” because he wasn’t beaten and the food was much better, though he described his interrogations as “very intense” and complained he was placed in solitary confinement and left handcuffed to a chain hanging from the ceiling one night in September 2003, which he assumed was punishment for telling an FBI agent that he was mistreated while in Medina.³⁸

On June 15, 2003, at the request of the U.S. government, the Mabahith allowed several officials from the FBI and the Secret Service to observe an

29. *Id.* at 345.

30. *Id.*

31. *Id.* at 367.

32. *Id.* at 368.

33. *Id.* at 346, 368–69.

34. *Id.* at 343. The statements were made on June 11, 12, and 15, and July 24, 2003. *Id.* at 346.

35. *Id.*

36. *Id.*

37. *Id.* at 347.

38. *Id.* at 369–70.

interrogation of Abu Ali through a two-way mirror.³⁹ The American officials observed while Saudi interrogators asked Abu Ali six of the thirteen questions requested by the FBI and Secret Service.⁴⁰ Meanwhile, in the United States, the FBI obtained and executed a search warrant at Abu Ali's home in Virginia on June 16, 2003.⁴¹

It is undisputed that Abu Ali remained in Saudi custody from the date of his capture—June 8, 2003—until February 21, 2005 and that he was repeatedly interrogated by the Mabahith while in custody—interrogations that included at least some questions provided by the FBI and Secret Service agents who were there to observe.⁴² Further, Abu Ali alleged that he was subjected on numerous occasions to torture and other coercive interrogation methods by his Saudi captors, although the bulk of his allegations would eventually be deemed not credible by the trial judge in his criminal case.⁴³

Nevertheless, in July 2004, Abu Ali's parents filed a habeas petition on his behalf in the U.S. District Court for the District of Columbia. Although Abu Ali was in Saudi custody, his parents claimed, *inter alia*, that the Saudis were detaining Abu Ali entirely at the behest of the U.S. government (and perhaps even to avoid the oversight of the U.S. courts); that U.S. officials were involved in Abu Ali's interrogation; that the Saudi government would immediately release Abu Ali to American officials upon a formal request from the U.S. government; and that Abu Ali was therefore in the "constructive custody" of the United States sufficient to trigger the jurisdictional provisions of the federal habeas statute.⁴⁴ The Government, rather than responding to Abu Ali's claims on the merits, moved to dismiss, arguing that the Supreme Court's 1948 decision in *Hirota v. MacArthur*⁴⁵ barred the district court from exercising jurisdiction.⁴⁶

In a thorough opinion handed down in December 2004, the district court denied the Government's motion to dismiss, holding that Abu Ali's

39. *Id.* at 343. In September 2003, the FBI was given a direct opportunity to interrogate Abu Ali. *Id.* Because none of the statements elicited during the September interview were introduced at trial, it did not factor into subsequent analysis of whether the summer interrogations were a joint venture. See *id.* at 382 (rejecting Ali's contention that the interrogation was a joint venture, partially because the government did not seek to use any of the September statements).

40. *Id.* at 350.

41. *United States v. Abu Ali*, 528 F.3d 210, 225 (4th Cir. 2008).

42. *Id.* at 224–25.

43. *Abu Ali*, 395 F. Supp. 2d at 375–79.

44. *Abu Ali v. Ashcroft*, 350 F. Supp. 2d 28, 30–31 (D.D.C. 2004).

45. 338 U.S. 197 (1948) (*per curiam*).

46. *Abu Ali*, 350 F. Supp. 2d at 31, 55. For a more thorough treatment of the relationship between *Abu Ali* and *Hirota*, see Stephen I. Vladeck, *Deconstructing Hirota: Habeas Corpus, Citizenship, and Article III*, 95 GEO. L.J. 1497, 1532–34 (2007). On the jurisdictional issue more generally, see Karen Shafir, *Habeas Corpus, Constructive Custody and the Future of Federal Jurisdiction After Munaf*, 16 U. MIAMI INT'L & COMP. L. REV. 91, 101–04 (2008) (discussing the district court's approach to habeas jurisdiction vis-à-vis *Hirota*).

allegations, if true, were sufficient to establish jurisdiction.⁴⁷ As Judge Bates explained,

The position advanced by the United States is sweeping. The authority sought would permit the executive, at his discretion, to deliver a United States citizen to a foreign country to avoid constitutional scrutiny, or, as is alleged and to some degree substantiated here, work through the intermediary of a foreign country to detain a United States citizen abroad.

The Court concludes that a citizen cannot be so easily separated from his constitutional rights. . . . Abu Ali was not captured on a battlefield or in a zone of hostilities—rather, he was arrested in a university classroom while taking an exam. The United States has therefore not invoked the executive’s war powers as a rationale for his detention—instead, the United States relies on the executive’s broad authority to conduct the foreign affairs of the country as a basis to insulate Abu Ali’s detention from judicial scrutiny. There are, to be sure, considerable and delicate principles of separation of powers that dictate caution and will narrow the inquiry in this case. Such principles, however, have never been read to extinguish the fundamental due process rights of a citizen of the United States to freedom from arbitrary detention at the will of the executive, and to access to the courts through the Great Writ of habeas corpus to challenge the legality of that detention.⁴⁸

Judge Bates proceeded to “authorize expeditious jurisdictional discovery . . . to further explore [Abu Ali’s] contentions.”⁴⁹ Such discovery never took place, though. Instead, six weeks after his ruling, on February 3, 2005, a federal grand jury in Alexandria, Virginia, returned an indictment against Abu Ali.⁵⁰ Shortly thereafter, Abu Ali was surrendered to U.S. authorities (perhaps vindicating one of the central claims of his habeas petition) and flown back to the United States, appearing in court for the first time on February 22, 2005—the day after he returned.⁵¹ Eventually, he was charged with nine distinct offenses: Conspiracy to Provide Material Support and Resources to a Designated Foreign Terrorist Organization (al Qaeda),⁵² Providing Material Support and Resources to a Designated Foreign Terrorist Organization (al Qaeda),⁵³ Conspiracy to Provide Material Support to Terrorists,⁵⁴ Providing Material Support to Terrorists,⁵⁵ Contribution of

47. *Abu Ali*, 350 F. Supp. 2d at 45–51; see also *id.* at 55–57 & n.26 (distinguishing *Hirota*).

48. *Id.* at 31 (internal citations omitted).

49. *Id.*

50. Indictment, *supra* note 14.

51. *United States v. Abu Ali*, 528 F.3d 210, 225 (4th Cir. 2008).

52. Indictment, *supra* note 14, at 1.

53. *Id.*

54. *Id.*

55. *Id.*

Services to al Qaeda,⁵⁶ Receipt of Funds and Services from al Qaeda,⁵⁷ Conspiracy to Assassinate the President of the United States,⁵⁸ Conspiracy to Commit Aircraft Piracy,⁵⁹ and Conspiracy to Destroy Aircraft.⁶⁰

In light of Abu Ali's transfer to U.S. custody and the indictment unsealed against him in the Eastern District of Virginia, Judge Bates ruled in September 2005 that Abu Ali's habeas petition had become moot.⁶¹ Although his opinion emphasized that "[n]othing in this opinion forecloses Abu Ali from pursuing whatever civil remedies may be available to him under the law for past wrongs,"⁶² he nevertheless concluded that Abu Ali no longer had a colorable claim for habeas relief.

B. *The Rule 15 Depositions*

Shortly after the indictment was filed, in March 2005, the Government moved under Rule 15 of the Federal Rules of Criminal Procedure for an order allowing it to depose Saudi witnesses—in particular Mabahith officers—in Saudi Arabia.⁶³ Over Abu Ali's objection, such depositions were taken in July 2005 using procedures that, whatever their merits, were certainly novel.⁶⁴ As the Fourth Circuit would later summarize,

As Saudi citizens who reside in Saudi Arabia, the Mabahith officers were beyond the subpoena power of the district court. Given this limitation, the United States government officially inquired into whether the Saudi Arabian government would allow the officers to testify at trial in the United States. The Saudi government denied this request, but permitted the officers to sit for depositions in Riyadh. As represented by counsel for the United States, this was a first in Saudi-American relations: the Saudi government had never before allowed such foreign access to a Mabahith officer.

Given the possibility of taking the deposition in Riyadh, the district court found it impractical for Abu Ali to travel to Saudi Arabia for two reasons. First, it would have been difficult for United States Marshals to maintain custody of Abu Ali while in Saudi Arabia Second, the fact that Abu Ali committed his offenses in Saudi Arabia might subject him to prosecution overseas, complicating—if not precluding—his return to the United States to face trial.⁶⁵

56. *Id.*

57. *Id.*

58. *United States v. Abu Ali*, 528 F.3d 210, 225 (4th Cir. 2008).

59. *Id.*

60. *Id.*

61. *Abu Ali v. Gonzales*, 387 F. Supp. 2d 16, 17 (D.D.C. 2005).

62. *Id.* at 20.

63. *Abu Ali*, 528 F.3d at 225.

64. *Id.*

65. *Id.* at 239.

In light of the practical obstacles, the district court sought to create deposition procedures that would protect Abu Ali's rights. Thus,

[a]t the court's directive, two defense attorneys, including Abu Ali's lead attorney, attended the depositions in Saudi Arabia, while a third attorney sat with Abu Ali in Virginia. Two attorneys for the government and a translator were also present in the room in Saudi Arabia while the Mabathith officers were being deposed.⁶⁶

Moreover, "[a] live, two-way video link was used to transmit the proceedings to a courtroom in Alexandria. This permitted Abu Ali and one of his attorneys to see and hear the testimony contemporaneously; it also allowed the Mabathith officers to see and hear Abu Ali as they testified."⁶⁷

To replicate normal conditions as best as possible, the testimony was transcribed by a court reporter in real time, and separate cameras recorded both the witnesses and Abu Ali, so that the jury could see their reactions.⁶⁸ Judge Lee presided from his courtroom in Alexandria, ruling on objections as they arose.⁶⁹ Finally, Abu Ali had the ability to communicate with his defense counsel in Saudi Arabia during the frequent breaks in the proceedings via cell phone.⁷⁰

Having fashioned these procedures, the district court presided over seven days of deposition testimony from several Saudi Mabathith officers involved in the arrest, detention, and interrogation of Abu Ali. The subject matter of the depositions encompassed all aspects of Abu Ali's experience with the Saudi criminal justice system, including the manner of his arrest, the length of his interrogation, the conditions of his confinement, the Mabathith's methods of questioning, and the circumstances surrounding his confessions.

....

Abu Ali's counsel actively participated throughout these depositions, objecting frequently during the government's direct examination and cross-examining each of the witnesses at length. In particular, Abu Ali's counsel were able to question the interrogating officers about Abu Ali's claims that he was tortured and beaten; deprived of sleep, food, and water; and denied use of a bathroom and mattress.⁷¹

66. *Id.* Judge Lee would later comment in an interview that, if he had it to do over again, he would have sent more than one translator. REAGAN, *supra* note 10, at 128 & nn.1092-93.

67. *Abu Ali*, 528 F.3d at 239.

68. *Id.* at 239-40.

69. *Id.*

70. *Id.*

71. *Id.* at 240.

C. *The Motions to Suppress and Dismiss*

Abu Ali next moved to suppress the admission of the Mabath officers' deposition testimony, along with various of the inculpatory statements he made while in Saudi custody, and for dismissal of the indictment.⁷² As the district court summarized the motion,

In his Motion to Suppress, Mr. Abu Ali asserts two principal arguments. First, he alleges that he was tortured while in Saudi custody and that the statements he allegedly made in detention are, therefore, involuntary and must be suppressed. Second, Mr. Abu Ali contends that the United States and the Saudi Government acted as partners or "joint venturers" in his arrest and lengthy detention in Saudi Arabia. He also argues that the Saudi government's search of his dormitory room in Medina and the search of his residence in Falls Church, Virginia, violated his Fourth Amendment rights against unreasonable searches and seizures. In his Motion to Dismiss, Mr. Abu Ali contends that because his arrest and lengthy detention were at the direction of the United States Government using the Saudi Arabia Government as a partner, joint venturer, or surrogate, the Indictment must be dismissed because the delay in his prosecution violates the Speedy Trial Act and his Sixth Amendment right to speedy trial.⁷³

After taking nearly two weeks of testimony in connection with Abu Ali's motions, the district court issued a painstaking 113-page opinion, concluding, in fine, that "the government has met its burden of proving that Mr. Abu Ali's statements were voluntary, and that the alleged defects in the aforementioned searches and Indictment do not violate Mr. Abu Ali's rights under the Fourth or Sixth Amendments."⁷⁴

With regard to Abu Ali's motion to suppress, the district court first concluded that Abu Ali's statements to the Saudi interrogators were voluntary, not the result of "gross abuse" or "inherently coercive conditions."⁷⁵ Despite recognizing that the voluntariness of the statements must be determined by the "totality of the circumstances,"⁷⁶ the court's discussion focused specifically on whether or not Abu Ali had been tortured.⁷⁷

The district court rested its holding that the statements were voluntary on the following four findings: (1) the Saudi lieutenant colonel, who was the warden at the Medina facility, represented that Abu Ali had not been tortured or questioned coercively in Medina and his testimony was held to be more

72. *United States v. Abu Ali*, 395 F. Supp. 2d 338, 341 (E.D. Va. 2005).

73. *Id.*

74. *Id.*

75. *Id.* at 373.

76. *Id.* at 372-73.

77. *Id.* at 386.

credible than Abu Ali's allegations that he had been tortured and abused; (2) the testimony of the Saudi captain and brigadier general, who both asserted that Abu Ali had not been tortured or abused while in custody at Riyadh and that Abu Ali did not appear to have been abused at the time they questioned him, was credible as well; (3) the testimony of both Saudi Arabian and American officials regarding Abu Ali's behavior throughout the period from June 11–15, 2003 was credible and did not coincide with the likely behavior a recently beaten person would exhibit; and (4) the testimony of Saudi and American officials also indicated that Abu Ali was concerned that the United States would find out he was in Saudi custody, and this concern raised serious questions about Abu Ali's claims of torture because "[i]t stretches credibility to think that a United States citizen who had just been beaten and tortured days before by foreign law enforcement officials would not want the United States to know that he was in custody abroad and was being tortured."⁷⁸

The court was also skeptical of Abu Ali's own account of his torture; it remarked that some aspects of his testimony "just do not flow logically"⁷⁹ and expressed apprehension over its inability to discern "whether Mr. Abu Ali is sincere or just cunning."⁸⁰ A particular point of contention was Abu Ali's inability to describe the object that hit him (even though he was blindfolded and chained to the floor), because, Judge Lee remarked, "it seems . . . that he could, at the very least, provide some basic description of what the item might have been based on how it felt to him."⁸¹ And based on its factual findings related to the conclusion that Abu Ali's statements were voluntary, the court further concluded that his treatment did not "shock[] the conscience."⁸²

Next, the district court turned to the *Miranda*⁸³ issue and whether the involvement of FBI and Secret Service agents in parts of Abu Ali's interrogation rendered it a "joint venture" to which *Miranda* would apply.⁸⁴

78. *Id.* at 374.

79. *Id.* at 378.

80. *Id.*

81. *Id.*

82. One might also view the competing testimony before the district court against the backdrop of the documented history (in U.S. State Department country reports) of abuses of detainees by the Saudi government—and the Mabahith in particular. See, e.g., Said, *supra* note 21, at 25–29 (criticizing the district court's unwillingness to take these reports into account). Even then, it is not at all obvious that the district court would have reached a different credibility determination, or would therefore have found Abu Ali's statements to have been involuntarily given. Nevertheless, in this regard, *Abu Ali* also highlights the difficulties of applying traditional "voluntariness" standards (let alone *Miranda* itself) to interrogations conducted overseas and by foreign officials. See *id.* at 4–7.

83. See *Miranda v. Arizona*, 384 U.S. 436, 444 (1966) (holding that the Fifth Amendment requires notice to the defendant of his right to counsel in a custodial interrogation in order to protect him from self-incrimination).

84. *Abu Ali*, 395 F. Supp. 2d at 381–83. On the joint venture doctrine, see *United States v. Yousef*, 327 F.3d 56, 145–46 (2d Cir. 2003) (requiring the suppression of statements elicited by

Based on the hearing testimony, the court concluded that “(1) U.S. law enforcement officials did not act in a ‘joint venture’ with Saudi officials in the arrest, detention; or interrogation of the defendant, and (2) Saudi law enforcement officials did not act as agents of U.S. law enforcement officials, and therefore *Miranda* warnings were not required.”⁸⁵

In arriving at this holding, the court did not define its understanding of “active” or “substantial” participation nor did it draw on comparisons from relevant case law.⁸⁶ Instead, Judge Lee concluded that the evidence clearly demonstrated that Saudi government officials arrested Abu Ali based on their own information and interest in interrogating him as a suspected member of a local terrorist cell, that the U.S. government did not learn of the defendant’s arrest until after it occurred, and that FBI agents were not present or involved with any of the interrogations prior to June 15, 2003—“when virtually all of the incriminating statements sought to be suppressed were made”—or on July 18 and 24, when the defendant hand wrote and videotaped his confession.⁸⁷

Although the court acknowledged that FBI and Secret Service agents *were* permitted to observe the June 15 interrogation (in which six out of the thirteen questions the FBI and Secret Service drafted were asked by the Saudi interrogators), it nevertheless concluded that “[t]he FBI and Secret Service were not allowed to determine the content or the form of the questions” asked during the interrogation.⁸⁸ And because of its conclusion that the interrogation was not a joint venture, the court similarly concluded that the Fourth Amendment simply did not apply to the search of Abu Ali’s dorm room in Medina.⁸⁹ As for the search of his parents’ home in Falls Church, Judge Lee concluded that the voluntary statements made by Abu Ali in his earlier interrogations provided more than sufficient probable cause.⁹⁰

The same analysis covered most of the grounds invoked by Abu Ali in his motion to dismiss. As for Abu Ali’s Speedy Trial Act claim, the court reiterated its finding that Abu Ali was arrested by the Saudi government for its own purposes and that Saudi officials did not act in a joint venture with, or as agents of, U.S. officials.⁹¹ Judge Lee was not persuaded by a U.S. State Department cable reporting a Saudi colonel’s statement that “‘Abu Ali could be rendered to American authorities at any time if the [U.S. government]

foreign police operating in the absence of *Miranda* protections where U.S. law enforcement agents actively participate in the questioning). *See also* *United States v. Bin Laden*, 132 F. Supp. 2d 168, 187 (S.D.N.Y. 2001) (recognizing the joint venture exception). *See generally* Said, *supra* note 21, at 10–12 & n.62 (summarizing the doctrine and citing relevant cases).

85. *Abu Ali*, 395 F. Supp. 2d at 381.

86. *Id.* at 381–83.

87. *Id.* at 381–82.

88. *Id.* at 382.

89. *Id.* at 383.

90. *Id.*

91. *Id.* at 384–85.

made a formal request,”⁹² because it “evinces little more than routine prosecutorial cooperation between two sovereigns,”⁹³ and because there was other evidence demonstrating that U.S. officials “specifically and expressly” requested that the defendant *not* be held merely on behalf of the U.S. government.⁹⁴ The court also found that Abu Ali’s Sixth Amendment right to a speedy trial did not attach until he was indicted or arrested and that he was not prejudiced by any pretrial delay that had taken place since the time of his indictment on federal charges on February 3, 2005, and his subsequent arrest on February 21, 2005.⁹⁵ Thus, the district court denied Abu Ali’s motions in their entirety.

D. *The CIPA Proceedings, Trial, and Sentencing*

At roughly the same time, the district court was also considering the Government’s request pursuant to the Classified Information Procedures Act (CIPA)⁹⁶ to introduce classified evidence at trial memorializing the communications between Sultan Jubran and Abu Ali.⁹⁷ Because Abu Ali’s chosen defense counsel did not possess security clearances (and were therefore not authorized to view classified documents), the district court appointed a CIPA-cleared attorney to assist in Abu Ali’s defense.⁹⁸ The Government first produced copies of the unredacted documents at issue to Abu Ali’s CIPA-cleared counsel on October 14, 2005, at which time it also informed her that the Government intended to introduce these documents at trial by proceeding through CIPA to seek “‘certain limitations on public disclosure that will be necessary to prevent the revelation of extremely sensitive national security information.’”⁹⁹ Three days later, the Government provided Abu Ali’s uncleared defense counsel with slightly redacted copies of the classified documents that had been provided to his CIPA-cleared counsel and informed Abu Ali and his counsel that the Government planned to “‘offer these communications into evidence at trial as proof that the defendant provided material support to al Qaeda.’”¹⁰⁰ As the Fourth Circuit would later explain, “the declassified versions provided the dates, the opening

92. *Id.* at 385.

93. *Id.*

94. *Id.*

95. *Id.* at 384.

96. *See* 18 U.S.C. app. 3 (2006) (detailing rules and procedures for the use of classified information in federal trials). Although CIPA applies on its face only to criminal trials, it has also been adopted in certain civil proceedings raising comparable considerations, especially habeas petitions arising out of the detention without charges of non-citizen terrorism suspects. *See, e.g.,* *Al Odah v. United States*, 559 F.3d 539, 544–47 (D.C. Cir. 2009); *In re Guantanamo Bay Detainee Litig.*, 634 F. Supp. 2d 17, 24 (D.D.C. 2009).

97. *United States v. Abu Ali*, 528 F.3d 210, 249 (4th Cir. 2008).

98. *Id.* at 248–49.

99. *Id.* at 249. Both of the communications at issue are excerpted in the Fourth Circuit’s opinion. *See id.*

100. *Id.*

salutations, the entire substance of the communications, and the closings, and had only been lightly redacted to omit certain identifying and forensic information.”¹⁰¹

On October 19, 2005, the Government filed an *in camera*, *ex parte* motion pursuant to section 4 of CIPA,¹⁰² seeking a protective order prohibiting testimony and lines of questioning that would lead to the disclosure of classified information contained in the documents memorializing the communications between Sultan Jubran and Abu Ali.¹⁰³ The district court curiously ruled that the Government could use the “silent witness” procedure to disclose classified information contained in these communications to the jury at trial,¹⁰⁴ even though Abu Ali himself would only be able to see the redacted version of the documents.¹⁰⁵ Abu Ali responded by filing a motion arguing that the Government must either declassify the documents in their entirety or that the court must order the Government to provide Abu Ali and his uncleared defense counsel the dates and manner in which the communications were obtained by the U.S. government.¹⁰⁶ The purpose of the request was apparently to ascertain whether the Government had discovered the existence of the communications prior to Abu Ali’s arrest by Saudi officials—which would presumably strengthen Abu Ali’s argument that his confessions to Saudi officials resulted from a “joint venture” with American law enforcement officers.¹⁰⁷

On October 21, the district court held an *in camera* CIPA hearing to consider Abu Ali’s motion.¹⁰⁸ At the hearing, the Government informed the court that although the communications were obtained prior to Abu Ali’s 2003 arrest in Saudi Arabia, they were obtained ““based on intelligence collect[ed] by the United States government with no involvement whatsoever of Saudi authorities.””¹⁰⁹ The district court concluded as a result that the communications were discovered independently from the Saudi government’s investigation (and were therefore not the product of a joint

101. *Id.*

102. 18 U.S.C. app. 3 § 4 (2006).

103. *United States v. Abu Ali*, 528 F.3d 210, 249–50 (4th Cir. 2008).

104. Under the “silent witness rule,”

the witness would not disclose the information from the classified document in open court. Instead, the witness would have a copy of the classified document before him. The court, counsel and the jury would also have copies of the classified document. The witness would refer to specific places in the document in response to questioning. The jury would then refer to the particular part of the document as the witness answered. By this method, the classified information would not be made public at trial but the defense would be able to present that classified information to the jury.

Id. at 250 n.18 (quoting *United States v. Zettl*, 835 F.2d 1059, 1063 (4th Cir. 1987)).

105. *Id.* at 250.

106. *Id.*

107. *Id.*

108. *Id.*

109. *Id.*

venture) and held that the redacted version of the documents provided to Abu Ali therefore “me[t] the defense’s need for access to the information.”¹¹⁰

During the trial, Abu Ali moved pursuant to section 5 of CIPA to allow his uncleared counsel to question the two witnesses the Government intended to call to introduce into evidence the substance of the classified communications in order to examine them “about their role in extracting, sharing, transferring, and handling [the] communications.”¹¹¹ The Government opposed the motion, contending that it would lead to the disclosure of classified information.¹¹² The district court then held another CIPA hearing, after which it concluded that Abu Ali’s rights under the Confrontation Clause were not infringed, because Abu Ali and his uncleared counsel “kn[e]w about and [were] given the substantive contents of the communications” and would “have the opportunity to cross-examine the communications carrier representative and the FBI agent regarding the substance of those communications.”¹¹³

Otherwise, Abu Ali’s trial proceeded largely without incident. On November 22, 2005, the jury returned a verdict convicting him on all charges.¹¹⁴ Judge Lee subsequently sentenced him to 360 months imprisonment, followed by a term of 360 months of supervised release.¹¹⁵ Abu Ali appealed his conviction and sentence to the Fourth Circuit; the Government cross-appealed his sentence.¹¹⁶

E. Appeal to the Fourth Circuit

On appeal, Abu Ali reiterated many of the claims he had advanced at trial. As relevant here,¹¹⁷ he first challenged the admission of his statements to the Saudi interrogators on the ground that they were involuntary and, in any event, were taken in violation of *Miranda*.¹¹⁸ Second, he argued that the Government failed adequately to corroborate his confessions.¹¹⁹ Third, Abu Ali claimed that the introduction of the Mabath officials’ deposition testimony violated his rights under the Sixth Amendment’s Confrontation Clause.¹²⁰ Fourth, Abu Ali challenged the Government’s introduction of classified evidence at trial (to which he was not privy) as a further violation

110. *Id.*

111. *Id.*

112. *Id.* at 251.

113. *Id.*

114. *Id.* at 226.

115. See *United States v. Abu Ali*, Crim. No. 05-53, 2006 WL 1102835, at *7 (E.D. Va. Apr. 17, 2006).

116. *Abu Ali*, 528 F.3d at 226.

117. For brevity’s sake, I have omitted several of Abu Ali’s additional claims on appeal that received summary treatment from the Fourth Circuit.

118. *Abu Ali*, 528 F.3d at 226.

119. *Id.* at 234.

120. *Id.* at 238.

of the Confrontation Clause.¹²¹ In an eighty-page, jointly authored opinion,¹²² Judges Wilkinson, Motz, and Traxler rejected nearly all of Abu Ali's arguments.¹²³

First, with regard to the *Miranda* issue, Judges Wilkinson and Traxler read prior precedent as establishing that "mere presence at an interrogation does not constitute the 'active' or 'substantial' participation necessary for a 'joint venture' but coordination and direction of an investigation or interrogation does."¹²⁴ Based on the findings made by the district court, the majority thereby affirmed Judge Lee's conclusion that Abu Ali's interrogation was not a joint venture and that the introduction of his statements at trial was therefore not a violation of *Miranda*.¹²⁵ As Judges Wilkinson and Traxler explained,

the Saudis were always in control of the investigation. It is clear to us, as it was to the district court, that the Mabahith never acted as a mouthpiece or mere conduit for their American counterparts. Based on these findings, we are convinced, as was the district court, that American law enforcement officials were not trying to evade the strictures of *Miranda*, and the June 15 interrogation did not rise to the level of a joint venture.¹²⁶

121. *Id.* at 254 n.21.

122. The only exceptions are footnotes five and six, the former of which spoke for Judges Wilkinson and Traxler on the *Miranda* joint venture issue, and the latter of which spoke for Judge Motz. *See id.* at 229-31 & nn.5-6.

123. *Id.* at 210-11. Judge Motz filed a separate dissent with regard to the majority's decision to vacate and remand Abu Ali's sentence. *Id.* at 269-82 (Motz, J., dissenting); *see also* Said, *supra* note 21, at 33-34 (noting the similarities between the majority's logic as to sentencing and its approach to the substantive issues Abu Ali raised on appeal).

124. *Abu Ali*, 528 F.3d at 229 n.5.

125. *Id.* at 229.

126. *Id.* at 230 n.5 (quoting *United States v. Martindale*, 790 F.2d 1129, 1131-32 (4th Cir. 1986)) (citation omitted). As the majority reasoned,

A determination that the suggestion of questions, without more, constitutes a joint venture would be problematic for at least two reasons. First, such a broad holding would contravene the well-established notion that *Miranda*, which is intended to regulate only the conduct of *American* law enforcement officers, does not apply extraterritorially to foreign officials absent significant involvement by American law enforcement. Second, such a broad per se holding could potentially discourage the United States and its allies from cooperating in criminal investigations of an international scope. Both the United States and foreign governments may be hesitant to engage in many forms of interaction if the mere submission of questions by a United States law enforcement officer were to trigger full *Miranda* protections for a suspect in a foreign country's custody and control. To impose all of the particulars of American criminal process upon foreign law enforcement agents goes too far in the direction of dictation, with all its attendant resentments and hostilities. Such an unwarranted hindrance to international cooperation would be especially troublesome in the global fight against terrorism, of which the present case is clearly a part.

Id. (citations omitted).

Judge Motz dissented on this point—the only trial-related issue that divided the otherwise united panel.¹²⁷ In her words,

Whatever else “active” or “substantial” participation may mean, when United States law enforcement officials propose the questions propounded by foreign law enforcement officials, and those questions are asked in the presence of, and in consultation with United States law enforcement officials, this must constitute “active” or “substantial” participation. After all, the purpose of an interrogation is to obtain answers to questions about criminal or otherwise dangerous activity. Drafting the questions posed to a suspect thus constitutes the quintessential participation in an interrogation. It differs in kind from observation of an interrogation, or rote translation of an interrogator’s questions and a suspect’s responses. Observers and translators undoubtedly gain important information from a suspect’s answers as well as from his behavior and demeanor, but those who formulate the questions asked during an interrogation actually direct the underlying investigation.¹²⁸

However, because Judge Motz agreed with Judges Wilkinson and Traxler that any error was harmless beyond a reasonable doubt,¹²⁹ the panel unanimously concluded that *Miranda* provided no basis for reversal. Similarly, the panel agreed with the district court that, separate from *Miranda*, Abu Ali had failed to demonstrate that his confessions were involuntary.¹³⁰ As such, the panel affirmed the district court’s denial of Abu Ali’s motion to suppress.¹³¹

Second, as to the independent corroboration issue, the Fourth Circuit conceded that the Government’s other evidence did not independently prove Abu Ali’s guilt.¹³² Nonetheless, the court explained that corroborating proof was sufficient so long as it “‘tend[ed] to establish’—not establish—‘the trustworthiness’ of the confession.”¹³³ The Government, according to the Fourth Circuit, “offered significant independent circumstantial evidence

127. *Id.* at 221.

128. *Id.* at 230 n.6 (citations omitted); *see also* Condon, *supra* note 21, at 680–84 (criticizing the narrowness of the *Abu Ali* majority’s joint-venture analysis). Although Judge Motz’s focus was on whether the interrogations were a “joint venture,” a closely related question, albeit one not raised in *Abu Ali*, is whether the traditional standards for “voluntariness” and “joint venture” analysis under *Miranda* should even *apply* where the relevant statements are made to foreign officials while in foreign custody (the *Abu Ali* court assumed without deciding that the answer was yes). For a detailed consideration of this complex issue, especially where non-citizens are concerned, *see In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 177, 198–215 (2d Cir. 2008). *See also* Said, *supra* note 21, at 14–15, 15 n.89 (discussing the Second Circuit’s analysis in *In re Terrorist Bombings*).

129. *See Abu Ali*, 528 F.3d at 231 (“*Abu Ali* had confessed to *each* of the crimes of which he was convicted before the June 15th interrogation took place. As a result, *Abu Ali*’s answers to the questions submitted by the FBI on June 15th were cumulative.”).

130. *Id.* at 231–34.

131. *Id.*

132. *Id.* at 236–37.

133. *Id.* at 237 (quoting *Opper v. United States*, 348 U.S. 84, 93 (1954)).

tending to establish the trustworthiness of Abu Ali's confessions."¹³⁴ In support, the court noted that the record included that evidence that an al Qaeda cell member identified Abu Ali as a member of the cell as well as documents containing two of Abu Ali's aliases recovered from the al Qaeda safe house and caches of weapons, explosives, cell phones, computers, and walkie-talkies found in the al Qaeda safe house (all of which Abu Ali had described in his confessions).¹³⁵ This evidence, as well as evidence gathered from Abu Ali's dormitory and home in Virginia, were held to corroborate Abu Ali's statements that he had "long wanted to join al Qaeda, to further its goals, and to provide it with support and assistance."¹³⁶ Moreover, according to the panel, "[p]erhaps the strongest independent evidence corroborating Abu Ali's confessions were two coded communications: one from him to Sultan Jubran occurring a day after the arrest of other cell members and the other from Sultan Jubran to him several days later."¹³⁷

Third, as to whether the ad hoc procedures devised for taking the deposition testimony of the Mabath officials violated Abu Ali's Confrontation Clause rights, the Fourth Circuit concluded that the district court's creative approach adequately protected Abu Ali.¹³⁸ Relying on the Supreme Court's decision in *Maryland v. Craig*,¹³⁹ the court of appeals concluded that the two conditions articulated in *Craig* for admitting testimony taken in the absence of the defendant—that the testimony in the defendant's absence be "necessary to further an important public policy," and that "the reliability of the testimony is otherwise assured"¹⁴⁰—were both met.

As to the first prong, the panel began with the observation that "[t]he prosecution of those bent on inflicting mass civilian casualties or assassinating high public officials is . . . just the kind of important public interest contemplated by the *Craig* decision."¹⁴¹ Moreover, "[i]f the government is flatly prohibited from deposing foreign officials anywhere but in the United States, this would jeopardize the government's ability to prosecute terrorists using the domestic criminal justice system."¹⁴² Thus, because "requiring face-to-face confrontation here would have precluded the government from relying on the Saudi officers' important testimony,"¹⁴³ the court held that the admission of the Mabath officials' deposition testimony satisfied the first prong of *Craig*.

134. *Id.* at 236.

135. *Id.*

136. *Id.*

137. *Id.*

138. *Id.* at 238–40.

139. 497 U.S. 836 (1990).

140. *Abu Ali*, 528 F.3d at 240–42 (quoting *Craig*, 497 U.S. at 850).

141. *Id.* at 241.

142. *Id.*

143. *Id.*

With regard to the second part of the *Craig* test, the court of appeals noted in detail the myriad steps the district court undertook to attempt to assure the reliability of the Mabath officials' testimony:

First, the Saudi witnesses testified under oath. While the oath used in this case, at the suggestion of defense counsel, was apparently an oath used in the Saudi criminal justice system, we cannot conclude, without more, that such an oath failed to serve its intended purpose of encouraging truth through solemnity. The oath used here was similar in most respects to the oath used in American judicial proceedings, and the appellant raised no objection to the oath in his briefs. Second, as discussed earlier, defense counsel was able to cross-examine the Mabath witnesses extensively. Finally, the defendant, judge, and jury were all able to observe the demeanor of the witnesses. Both the defendant and the judge were able to view the witnesses as they testified via two-way video link, and the jury watched a videotape of the deposition at trial. This videotape presented side-by-side footage of the Mabath officers testifying and the defendant's simultaneous reactions to the testimony.¹⁴⁴

Thus, the panel unanimously concluded that the *Craig* standard was satisfied and that Abu Ali's Confrontation Clause rights were not violated by the introduction at trial of the Mabath officials' deposition testimony.¹⁴⁵

Finally, the panel turned to the Confrontation Clause error at trial—the disclosure to the jury via the “silent witness” procedure of classified information (the documents memorializing communications between Sultan Jubran and Abu Ali following the May 2003 Mabath raids in Medina) where Abu Ali had received only the redacted, unclassified version of the documents.¹⁴⁶ As the court explained,

The error in the case, which appears to have originated in the October 2005 CIPA proceeding, was that CIPA was taken one step too far. The district court did not abuse its discretion in protecting the classified information from disclosure to Abu Ali and his uncleared counsel, in approving a suitable substitute, or in determining that Abu Ali would receive a fair trial in the absence of such disclosure. But, for reasons that remain somewhat unclear to us, the district court

144. *Id.* at 241–42. For criticism of this analysis, see Said, *supra* note 21, at 31 & n.230.

145. *Abu Ali*, 528 F.3d at 242. In a footnote, the Fourth Circuit distinguished the Eleventh Circuit's recent decision in *United States v. Yates*, 438 F.3d 1307 (11th Cir. 2006) (en banc). *Abu Ali*, 528 F.3d at 242 n.12. *Yates* held that a defendant's Confrontation Clause rights were violated when a witness was allowed to testify at trial via a live two-way video link from Australia. 438 F.3d at 1310, 1319. As the *Abu Ali* court explained, “Whatever the merits of the holding in *Yates*, the defendants there were charged with mail fraud, conspiracy to commit money laundering, and drug-related offenses, crimes different in both kind and degree from those implicating the national security interests here.” 528 F.3d at 242 n.12 (citation omitted). Moreover, unlike Judge Lee, the district court in *Yates* had failed “to consider potential alternatives that would have enabled the witnesses to testify face-to-face with the defendant.” *Id.*

146. *Abu Ali*, 528 F.3d at 244.

granted the government's request that the complete, unredacted classified document could be presented to the jury via the "silent witness" procedure. The end result, therefore, was that the jury was privy to the information that was withheld from Abu Ali.¹⁴⁷

Concluding that the silent witness procedure is meant to keep classified information from the *public*, but not the defendant, the panel noted that "CIPA does not . . . authorize courts to provide classified documents to the jury when only such substitutions are provided to the defendant."¹⁴⁸ Moreover, there was no room to "balance a criminal defendant's right to see the evidence which will be used to convict him against the government's interest in protecting that evidence from public disclosure."¹⁴⁹ Instead,

[i]f the government does not want the defendant to be privy to information that is classified, it may either declassify the document, seek approval of an effective substitute, or forego its use altogether. What the government cannot do is hide the evidence from the defendant, but give it to the jury.¹⁵⁰

By so acting, the Government violated Abu Ali's Confrontation Clause rights.¹⁵¹

Nevertheless, the panel concluded that the district court's error (and the concomitant violation of the Confrontation Clause) were harmless.¹⁵² Abu Ali and his uncleared counsel were given copies of the declassified versions of the communications well in advance of trial, and there was no information in the classified versions that, according to the court of appeals, they would not have already prepared for in considering the declassified versions.¹⁵³ Instead, "the information that had been redacted from the declassified version was largely cumulative to Abu Ali's own confessions and the evidence discovered during the safe house raids, which were presented to the jury."¹⁵⁴

Having thereby affirmed Abu Ali's conviction, Judges Wilkinson and Traxler turned to the Government's cross-appeal of Abu Ali's sentence, concluding that the district court erred in relying on comparisons to "similar" cases in applying a downward deviation from Abu Ali's presumptive sentence under the Federal Sentencing Guidelines—that Abu Ali's sentence was unreasonably lenient.¹⁵⁵ Although the majority left it up to the district court

147. *Id.* at 254.

148. *Id.* at 255; *see also id.* ("There is a stark difference between *ex parte* submissions from prosecutors which protect the disclosure of irrelevant, nonexculpatory, or privileged information, and situations in which the government seeks to use *ex parte* information in court as evidence to obtain a conviction.")

149. *Id.*

150. *Id.*

151. *Id.*

152. *Id.* at 256.

153. *Id.* at 256–57.

154. *Id.* at 257.

155. *Id.* at 261–65, 269.

to resentence on remand, it stressed that the sentence should “reflect the full gravity of the situation before us.”¹⁵⁶

Judge Motz dissented with regard to sentencing, arguing that the majority was misapplying the Supreme Court’s recent decisions in *Gall v. United States*¹⁵⁷ and *Kimbrough v. United States*,¹⁵⁸ both of which, in clarifying the proper scope of appellate review after *United States v. Booker*,¹⁵⁹ compelled deference to the district court’s reasonable justifications for applying a downward deviation.¹⁶⁰ Instead, Judge Motz concluded, the majority opinion “reject[ed] the central lesson from [these cases] that reviewing courts owe deference to *both* the overall sentence selected by the district court *and* the justifications given for that sentence. Proper application of this deferential abuse of discretion standard requires affirmance.”¹⁶¹

F. *Petition for Certiorari*

Notwithstanding the numerous significant legal issues implicated by the district court’s and the Fourth Circuit’s decisions, Abu Ali’s subsequent petition for a writ of certiorari to the Supreme Court raised only the Confrontation Clause error and whether such Sixth Amendment violations could *ever* be harmless.¹⁶² Thus, the petition argued that a “defendant’s right to view the prosecution’s evidence admitted against him at trial is so fundamental to the Sixth Amendment right to confrontation that it” should not be subject to harmless error review.¹⁶³ The Fourth Circuit’s reliance on *Delaware v. Van Arsdall*¹⁶⁴ to apply harmless error review, the petition maintained, was inapposite, because “*Van Arsdall* involved a matter the federal rules . . . place firmly within the District Court’s discretion—the scope and extent of cross-examination.”¹⁶⁵ Here, in contrast, the issue was the trial court’s “authority to pick and choose what evidence admitted at trial the defendant will be permitted to see at all” and “not the trial court’s discretion to manage cross-examination.”¹⁶⁶

156. *Id.* at 269.

157. 552 U.S. 38 (2007).

158. 552 U.S. 85 (2007).

159. 543 U.S. 220 (2005).

160. *Abu Ali*, 528 F.3d at 272–73 (Motz, J., dissenting). See generally Lindsay C. Harrison, *Appellate Discretion and Sentencing After Booker*, 62 U. MIAMI L. REV. 1115 (2008) (summarizing the particular issues raised by appellate review of district court decisions after *Booker*).

161. *Abu Ali*, 528 F.3d at 282 (Motz, J., dissenting).

162. *Petition for Writ of Certiorari*, *supra* note 19, at i, 23.

163. *Id.* at 17.

164. 475 U.S. 673 (1986); see also *id.* at 681–84 (describing the appropriateness of harmless error review for certain Confrontation Clause errors).

165. *Petition for Writ of Certiorari*, *supra* note 19, at 22–23.

166. *Id.* at 23. More generally, the petition repeatedly alluded to the point that it was difficult to square at least some of the Fourth Circuit’s Confrontation Clause analysis with the Supreme Court’s paradigm-shifting decision in *Crawford v. Washington*, 541 U.S. 36 (2004). See, e.g., *Petition for Writ of Certiorari*, *supra* note 19, at 19 (noting that Abu Ali was denied “personal

Moreover, the petition argued, CIPA should not have any bearing on the harmless error analysis, because nothing in CIPA “contemplates the government’s disclosure of classified information to the jury and not the defendant.”¹⁶⁷ Further, allowing harmless error review of the Confrontation Clause violation would place defendants such as Abu Ali in an untenable position: how could one possibly demonstrate prejudice or rebut the Government’s claim of harmlessness when he has not seen the evidence in question?¹⁶⁸ Instead, the petition urged the Supreme Court to use *Abu Ali* to create a bright-line rule, arguing that harmless error analysis will produce a case-by-case analysis that will threaten fundamental Sixth Amendment principles and lead to the “incremental but inexorable erosion of the confrontation right.”¹⁶⁹

Without comment or dissent, the Supreme Court denied certiorari on February 23, 2009.¹⁷⁰ On remand to the district court for resentencing, Judge Lee resentenced Abu Ali to life in prison,¹⁷¹ which Abu Ali has again appealed to the Fourth Circuit.¹⁷² Short of a surprising change of direction from the Court of Appeals on the sentencing issue, however, his legal proceedings are likely to come to a close.

Before turning to the three hard substantive questions that *Abu Ali* raises with implications for future cases, it is worth pausing for a moment to note the Fourth Circuit’s own rhetoric in disposing of Abu Ali’s claims on appeal. Although the court at various points relied upon the serious (and terrorism-based) nature of the charges against Abu Ali (as, for example, in its discussion of the policy interest in allowing deposition testimony outside the defendant’s presence), it seemed just as sensitive to the significance of civilian criminal process in such cases as a general matter.¹⁷³ As the panel noted at the outset of its opinion,

Unlike some others suspected of terrorist acts and designs upon the United States, Abu Ali was formally charged and tried according to the customary processes of the criminal justice system. Persons of good will may disagree over the precise extent to which the formal criminal justice process must be utilized when those suspected of

examination’ entirely with respect to the redacted portions” of the evidence (quoting *Crawford*, 541 U.S. at 49–50)).

167. Petition for Writ of Certiorari, *supra* note 19, at 24.

168. *Id.* at 26–27.

169. *Id.* at 29.

170. *Abu Ali v. United States*, 129 S. Ct. 1312 (2009).

171. Jerry Markon, *Falls Church Man’s Sentence in Terror Plot Is Increased to Life*, WASH. POST, July 28, 2009, at A3.

172. See Docket Sheet, *United States v. Abu Ali*, No. 09-4705 (4th Cir. Aug. 3, 2009) (noting oral argument scheduled for May 2010).

173. See *United States v. Abu Ali*, 528 F.3d 210, 256 (4th Cir. 2008) (recognizing that the criminal process focuses on the “fairness of the trial” (quoting *Delaware v. Van Arsdaal*, 475 U.S. 673, 681 (1986))).

participation in terrorist cells and networks are involved. There should be no disagreement, however, that the criminal justice system does retain an important place in the ongoing effort to deter and punish terrorist acts without the sacrifice of American constitutional norms and bedrock values. As will be apparent herein, the criminal justice system is not without those attributes of adaptation that will permit it to function in the post-9/11 world. These adaptations, however, need not and must not come at the expense of the requirement that an accused receive a fundamentally fair trial.¹⁷⁴

The sentiment is admirable. But the question remains whether the district and circuit courts' adaptations in *Abu Ali*'s case appropriately struck this balance: permitting the civilian courts to function in the post-9/11 world while not coming at the expense of *Abu Ali*'s right to a fair trial. It is to this—harder—matter that this Article now turns.

II. The Three Hard Questions Raised by *Abu Ali*

As noted above, although *Abu Ali*'s trial and appeal raised a number of legal issues, three stand out as particularly interesting and unique: (1) the hybrid and ad hoc procedures that the district court fashioned in order to allow for the deposition testimony of the Mabath officials, (2) the *Miranda*“joint venture” question and the Fourth Circuit's divided approach to that issue, and (3) the CIPA/Confrontation Clause error and the question of whether such errors really can be harmless.¹⁷⁵ As the following discussion suggests, what these issues have in common is the extent to which their resolution simultaneously demonstrates the flexibility that federal courts can exercise in these cases and the potential dangers lurking in the background for the rights of defendants.

A. *The Mabath Officials' Deposition Testimony and Rule 15 of the Federal Rules of Criminal Procedure*

In its current form, Rule 15 of the Federal Rules of Criminal Procedure requires the presence of a defendant who is “in custody” at any pretrial deposition, except where the defendant waives his right to be present or “persists in disruptive conduct justifying exclusion after being warned by the court that disruptive conduct will result in the defendant's exclusion.”¹⁷⁶ As cases like *Abu Ali* demonstrate, though, it is increasingly likely that circumstances will arise in which it is impossible to simultaneously secure the testimony of individuals outside the United States while guaranteeing the presence of the defendant.¹⁷⁷ Thus, courts have increasingly recognized

174. *Id.* at 221.

175. See *supra* notes 13–19 and accompanying text.

176. FED. R. CRIM. P. 15(c)(1).

177. See *Abu Ali*, 528 F.3d at 239 (explaining that (1) Mabath officers were Saudi citizens residing in Saudi Arabia outside the subpoena power of the U.S. district court and were only

circumstances—such as those in *Abu Ali*—where depositions taken outside the defendant’s presence do not violate the Confrontation Clause.¹⁷⁸

Mindful of these concerns, the Advisory Committee on Federal Rules of Criminal Procedure has proposed a revision to Rule 15 that would allow depositions outside the defendant’s presence whenever a trial court finds

- (1) the witness’s testimony could provide substantial proof of a material fact in a felony prosecution;
- (2) there is a substantial likelihood the witness’s attendance at trial cannot be obtained;
- (3) the defendant cannot be present at the deposition or it would not be possible to securely transport the defendant to the witness’s location for a deposition; and
- (4) the defendant can meaningfully participate in the deposition through reasonable means.¹⁷⁹

The proposed revision, though, raises both practical and constitutional concerns, as a trio of Latham & Watkins lawyers have demonstrated in an insightful recent article.¹⁸⁰ In particular, the new rule would run roughshod over the requirement articulated in *Craig* that testimony taken outside the defendant’s presence be “necessary to further an important public policy.”¹⁸¹ Although one may well be convinced by the Fourth Circuit’s analysis in *Abu Ali* that the ability effectively to prosecute crimes related to transnational terrorism is an important public policy that would justify the accommodation,¹⁸² it is not at all clear that the same argument would hold for lesser crimes—even if they are felonies, as the new rule would provide.¹⁸³ Indeed, that concern was at the heart of the en banc Eleventh Circuit’s decision in the *Yates*

permitted by the Saudi government to have their depositions taken in Riyadh, not in the United States, and (2) it would be impractical for the defendant to be physically present for Rule 15 depositions taken in Saudi Arabia because “it would have been difficult for United States Marshals to maintain custody of [the defendant] while in Saudi Arabia” and because there was a serious risk that Saudi officials would attempt to prosecute him themselves since the defendant committed his offenses in Saudi Arabia, “complicating—if not precluding—his return to the United States to face trial”).

178. See, e.g., *id.* at 238 n.11 (citing federal courts of appeals cases where Rule 15 depositions of foreign witnesses taken when the defendant was not present were allowed into evidence).

179. CONFERENCE COMM. ON RULES OF PRACTICE AND PROCEDURE, JUDICIAL CONFERENCE, SUMMARY OF THE REPORT OF THE JUDICIAL CONFERENCE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE 20–21 (2009).

180. Sabin et al., *supra* note 15, at 35 (suggesting that the proposed rule would be attacked as a violation of the Sixth Amendment’s Confrontation Clause, especially as it relates to the cross-examination of foreign witnesses).

181. *Maryland v. Craig*, 497 U.S. 836, 850 (1990); see also Sabin et al., *supra* note 15, at 38 (observing that because “amended Rule 15 would permit foreign deposition testimony for all transnational crimes,” it would not be limited to cases involving sufficiently important public policies).

182. Even still, critics have noted that such an accommodation nevertheless removes the possibility of perjury as a counterweight to untruthful testimony, and may therefore render such testimony inherently unreliable. See, e.g., Said, *supra* note 21, at 31 & n.230 (noting the lack of impediments to engage in perjury in *Abu Ali*’s trial).

183. See Sabin et al., *supra* note 15, at 38 (contending that “[a]s case law makes clear, national security is a sufficiently important public policy to justify two-way video testimony, but it is a high bar and other policies are likely to fail”).

case, cited and distinguished in *Abu Ali*.¹⁸⁴ As the Latham & Watkins lawyers explain, “Unless limitations are placed on this potentially sweeping category of federal crimes, the concerns articulated by the *Yates* court—a lack of specific factual findings and insufficiently important public policies—will be realized.”¹⁸⁵ Thus, the authors instead cite with approval Judge Lee’s painstaking accommodations in *Abu Ali*, noting both the specific findings of an important public policy and the myriad steps Judge Lee took to preserve the reliability of the testimony.¹⁸⁶ Lee’s procedures, they note, are a model in both form and substance, since they recognize the need to accommodate the foreign witnesses while adopting unprecedented protections for the defendant and his counsel.¹⁸⁷

Equally significant, though, is a separate point made by the Latham & Watkins lawyers in their critique of the proposed revisions to Rule 15: as technology improves, the confrontation issues that such remote and impersonal depositions might raise could largely subside.¹⁸⁸ Thus, as they note with regard to just one example,

[T]elepresence is a relatively new technology capable of full-duplex, high-definition, immersive video conferencing. The premise behind this new generation of video conferencing is that the experience should emulate as much as possible the experience of sitting across a table from the other party, to the point that some telepresence systems forego a mute button. The picture is 1080p full high-definition, there is little or no sound delay, and it includes the capability to show a document directly to the opposing side in realtime. Telepresence further reduces the distinction between virtual and in-person confrontation. Conversely, video testimony may actually improve other senses by, for example, zooming in on the witness’s face or amplifying sounds. As telepresence becomes more accessible and the technology continues to improve, the drawbacks of two-way video depositions decrease significantly.¹⁸⁹

This point may seem simplistic, but when tied together with *Abu Ali*, it shows how a combination of judicial creativity and technological advancement can help courts strike the balance between the defendant’s right to confront the witnesses against him and the unique logistical impediments that can arise when prosecuting complex transnational terrorism cases. *Abu Ali* may well have struck the appropriate balance, but only because of the case-specific accommodations made by the trial court.

184. *United States v. Abu Ali*, 528 F.3d 210, 242 n.12 (4th Cir. 2008).

185. Sabin et al., *supra* note 15, at 38.

186. *Id.* at 36–37.

187. *See id.* at 34–37 (arguing that Rule 15 should incorporate the *Abu Ali* procedures since they can be used to satisfy Sixth Amendment Confrontation Clause concerns even when foreign witnesses are unable to travel to the United States).

188. *Id.* at 38.

189. *Id.*

B. The Battle of the Footnotes: Miranda and the “Joint Venture”

Perhaps the most controversial aspect of the *Abu Ali* litigation was the joint venture issue—whether U.S. officials were sufficiently involved in Abu Ali’s interrogations at the hands of the Mabahith such that *Miranda* should have applied to preclude the admission of Abu Ali’s inculpatory statements at trial.¹⁹⁰ Moreover, and unlike the sui generis deposition and CIPA issues that characterized Abu Ali’s trial, the question of when and to what extent *Miranda* is triggered by overseas interrogations of individuals in some form of joint custody is likely to be one that will recur time and again in the ensuing years.

To recap, the Fourth Circuit panel in *Abu Ali* split on the substance of this issue, although they agreed that any *Miranda* error was harmless.¹⁹¹ On the merits, Judges Wilkinson and Traxler concluded that the critical fact was that

the Mabahith “determined what questions would be asked, determined the form of the questions, and set the length of the interrogation.” In fact, the Saudi interrogators refused to ask a majority of the questions submitted by the United States, and asked a number of their own questions during the interrogation.¹⁹²

Thus, “we are convinced, as was the district court, that American law enforcement officials were not trying to ‘evade the strictures of *Miranda*.’”¹⁹³ Judge Motz, in contrast, believed that the critical fact was that questions presented by U.S. officials were answered by the defendant.¹⁹⁴ Or, as she put it, “when United States law enforcement officers provide the questions to be asked of a suspect by cooperating foreign law enforcement officials, they clearly have engaged in ‘active’ or ‘substantial’ participation such that any resultant interrogation becomes a joint venture.”¹⁹⁵

To be sure, it bears emphasizing that the two footnotes are fighting over inches of jurisprudential real estate. But the inches are significant. The question presented in *Abu Ali* was unprecedented, since no prior reported decision involved U.S. officials submitting questions specifically to be asked of U.S. citizens by foreign interrogators on foreign soil.¹⁹⁶ And so the ques-

190. *United States v. Abu Ali*, 528 F.3d 210, 228 (4th Cir. 2008) (“The ‘joint venture’ doctrine provides that ‘statements elicited during overseas interrogation by foreign police in the absence of *Miranda* warnings must be suppressed whenever United States law enforcement agents actively participate in questioning conducted by foreign authorities.’”).

191. *Id.* at 229–31 & nn.5–6.

192. *Id.* at 229–30 n.5.

193. *Id.* at 230 n.5.

194. *Id.* at 231 n.6 (stating that drafting the questions to be posed to the suspect during an interrogation “constitutes the quintessential participation” in the interrogation).

195. *Id.*

196. *See id.* at 228 (noting, in review of previous cases involving the joint venture doctrine, none of which are directly on point, that “[o]nly a few cases illuminate what constitutes ‘active’ or ‘substantial’ participation”).

tion really reduces to formalism versus functionalism—do the U.S. officials actually have to play a formal role in *running* the interrogation to trigger the “joint venture” doctrine or is it enough that the interrogation *includes* questions that, but for the U.S. involvement, the foreign interrogators might not have asked?

To their credit, both sides marshaled forceful policy arguments in support of their view. Thus, Judges Wilkinson and Traxler emphasized that

such a broad per se holding [requiring *Miranda* protection] could potentially discourage the United States and its allies from cooperating in criminal investigations of an international scope. Both the United States and foreign governments may be hesitant to engage in many forms of interaction if the mere submission of questions by a United States law enforcement officer were to trigger full *Miranda* protections for a suspect in a foreign country’s custody and control. To impose all of the particulars of American criminal process upon foreign law enforcement agents goes too far in the direction of dictation, with all its attendant resentments and hostilities. Such an unwarranted hindrance to international cooperation would be especially troublesome in the global fight against terrorism, of which the present case is clearly a part.¹⁹⁷

Not to be outdone, Judge Motz emphasized how the majority’s view “permits United States law enforcement officers to strip United States citizens abroad of their constitutional rights simply by having foreign law enforcement officers ask the questions. This cannot be the law.”¹⁹⁸

The answer may well be somewhere in between; a formal rule requiring *Miranda* whenever U.S. officials submit questions to foreign interrogators may well have the chilling effect described by Judges Wilkinson and Traxler, and an equally formal rule *not* requiring *Miranda* unless U.S. officials are actually *running* the interrogation may create the perverse incentives identified by Judge Motz. Instead, the question may well need to turn on the motive of the U.S. officials, notwithstanding the Court’s increasing hostility toward subjective tests in the context of criminal procedure jurisprudence.¹⁹⁹

197. *Id.* at 230 n.5. Of course, that concern is only raised if and when the United States seeks both (1) to prosecute the detainee and (2) to admit statements made during the overseas interrogation. Obviously, *Miranda* has no bearing on cases where the detainee is never charged in an American court or where, even if he is, his statements while in foreign detention are not introduced at trial. See *United States v. Francis*, 542 U.S. 630, 637–38 (2004) (noting that coverage of the protection afforded by the Fifth Amendment’s Self-Incrimination Clause, which the *Miranda* rule is designed to safeguard, is limited to compelled testimony that is used against the defendant in a criminal proceeding).

198. *Abu Ali*, 528 F.3d at 231 n.6.

199. For example, consider the Court’s otherwise-fractured decision in *Missouri v. Seibert*, 542 U.S. 600 (2004), in which eight of the nine Justices—all except Justice Kennedy—rejected a focus on the subjective intent of the interrogating officer in deciding the admissibility of statements made after a “midstream” *Miranda* warning.

But either way, perhaps the larger point to take away is that the *Miranda* issue in *Abu Ali* is not unique to terrorism cases. Although it is probably safe to conjecture that a disproportionately high percentage of cases in which this issue arises will involve terrorism-related charges, the merits of the legal question are in no way tied to any consideration of the underlying offense.²⁰⁰ Put another way, the rhetoric of Judges Wilkinson and Traxler notwithstanding, foreign interrogations of U.S. citizens raise complicated *Miranda* questions (and always have) whether or not the citizen is suspected of terrorism-related offenses. Thus, and unlike the Rule 15 issue presented in *Abu Ali*, which turned to a large degree on the government's case-specific policy interests, the *Miranda* issue is usefully capable of generalization; put differently, whatever the answer, there is less risk of "seepage" here.

C. *The Confrontation Clause Error and Its Harmlessness*

Last, we come to the one error with regard to which everyone is in agreement: the district court's surprising and unjustified use of the "silent witness" procedure at trial, pursuant to which the jury was privy to classified information even though the defendant had access only to the redacted, declassified version.²⁰¹ In one sense, the error was usefully small: the portion of the communications to which Abu Ali lacked access did not go to their substance, but rather to identifying information that may have bolstered Abu Ali's claim that the Government had learned of their existence prior to his arrest, which would further support his "joint venture" argument.²⁰² Nevertheless, the Fourth Circuit was unequivocal in concluding that the introduction of such evidence was necessarily a violation of Abu Ali's Confrontation Clause rights, albeit one that the other evidence against him rendered harmless.²⁰³

Unless one is taken by Abu Ali's argument in his petition for certiorari that certain Confrontation Clause claims should not be subject to harmless error analysis—an argument that runs against a substantial body of precedent—the real lesson from this aspect of the *Abu Ali* litigation may just be that while mistakes will be made, the Supreme Court's increasing embrace of harmless error principles heavily mitigates the consequences of

200. See, e.g., Andreas F. Lowenfeld, *U.S. Law Enforcement Abroad: The Constitution and International Law, Continued*, 84 AM. J. INT'L L. 444, 459 (1990) (noting the increasing involvement across the board of U.S. officials in foreign law enforcement investigations, and the potential in those contexts for abuse of traditional constitutional protections).

201. *Abu Ali*, 528 F.3d at 255.

202. As the Government succinctly pointed out in its brief in opposition to certiorari, the error did not in any way advance Abu Ali's claim that there was insufficient evidence to corroborate his confessions, even though the classified communications were "[p]erhaps the strongest independent evidence" thereto. Brief for the United States in Opposition at 17 n.5, *United States v. Abu Ali*, 129 S. Ct. 1312 (2009) (No. 08-064). After all, the *substance* of the communications was *not* classified; only certain identifying and forensic information was redacted. *Id.*

203. *Abu Ali*, 528 F.3d at 255–56.

those mistakes. Indeed, it was harmless error that created consensus on the *Abu Ali* panel with regard to the *Miranda* issue, and it was harmless error that rendered the Confrontation Clause violation a non-issue as well.²⁰⁴ In that regard, it is telling that *Abu Ali*'s petition for certiorari did not challenge the Fourth Circuit's conclusion that the Confrontation Clause error was harmless; it challenged whether, categorically, it *could* be.²⁰⁵

Any number of scholars have wondered whether the Supreme Court in recent years has taken the harmless error doctrine too far.²⁰⁶ But leaving that debate for another day, it seems clear that, as with the *Miranda* issue in *Abu Ali*, the harmless error question does not in any meaningful way turn on the centrality of terrorism and national security concerns in the litigation. That would change, of course, if the Government's violation of the Confrontation Clause was *not* harmless, but in a way, that proves the point. After all, the flaw in *Abu Ali*'s case with regard to the silent witness procedure was *not* that the law failed to provide adequate means of balancing the government's national security interests with the defendant's right to a fair trial; the flaw was that the trial court, for whatever reason, failed to follow the law.²⁰⁷

III. Conclusion: Terrorism Trials After *Abu Ali*

In sum, then, *Abu Ali* emerges as an unvarnished example of how the civilian criminal justice system can handle high-profile criminal terrorism cases raising novel logistical, procedural, and substantive challenges. The thoughtful procedure devised by Judge Lee to allow the Mabath officials to testify while protecting the defendant's Confrontation Clause rights are a model that courts should follow (and *have* followed²⁰⁸), and more generally demonstrates the ways in which courtroom technology and a focus on the specific national security implications of a trial can actually help *cabin* proposed changes to the Federal Rules of Criminal Procedure in a manner that is more protective of individual defendants' rights. The principled disagreement over whether *Abu Ali*'s interrogation constituted a "joint venture" raises an important and contested question of constitutional criminal procedure that turns in no meaningful substantive way on the fact that his was a

204. *Id.* at 257.

205. See Petition for Writ of Certiorari, *supra* note 19, at 29 (arguing that the application of harmless error to the Sixth Amendment violation would allow "incremental but inexorable erosion of the confrontation right through case-by-case analysis").

206. See, e.g., Charles S. Chapel, *The Irony of Harmless Error*, 51 OKLA. L. REV. 501, 521–28 (1998) (discussing the patchwork development of the harmless error rule and critiquing its application); Jeffrey O. Cooper, *Searching for Harmlessness: Method and Madness in the Supreme Court's Harmless Constitutional Error Doctrine*, 50 U. KAN. L. REV. 309, 345–46 (2002) (arguing against the current approach and proposing one that is more protective of constitutional and individual rights).

207. See *Abu Ali*, 528 F.3d at 255 ("The error in the case . . . was that CIPA was taken one step too far.")

208. See, e.g., *United States v. Ahmed*, 587 F. Supp. 2d 853, 854–55 (N.D. Ohio 2008) (endorsing the *Abu Ali* procedure).

terrorism trial, as opposed to a trial for any other offense over which the federal courts have jurisdiction. And the clear Confrontation Clause violation resulting from the trial court's use of the "silent witness" rule shows both the settling effect of harmless error doctrine and the extent to which procedural flaws sometimes derive not from the laws but from the judges who apply them.

None of these points, on their own, do anything conclusively to establish the feasibility of civilian criminal trials for *all* terrorism suspects, including the 9/11 defendants. If *Abu Ali* proves anything, it proves that every case raises its own unique set of practical, procedural, and substantive challenges. But perhaps it proves a bit more: where unique national security concerns are implicated, *Abu Ali* suggests that courts *will* attempt to reach accommodations that take into account both the Government's interest and the fundamental protections to which defendants are entitled, keeping in mind Justice Frankfurter's age-old admonition that "the safeguards of liberty have frequently been forged in controversies involving not very nice people."²⁰⁹ But even in terrorism cases, *Abu Ali* suggests that courts are also able faithfully to apply extant precedents that *don't* turn on the government's unique interests, even if they disagree about the substantive answer—that some doctrines are usefully insulated from the danger of seepage. And *Abu Ali* reminds us that sometimes, the law *is* set up properly to resolve the tension between the government's interests and the defendant's rights; it is just that the judges get it wrong.

But what *Abu Ali* might drive home the most forcefully is just how seriously Article III judges from across the political spectrum take their responsibility in these cases—not just to the litigants but to their institution and its posterity. I suspect that Judges Wilkinson, Motz, and Traxler meant to pay far more than lip service to this idea in the opening pages of their joint opinion for the Fourth Circuit, where, in one voice, they emphasized that "[t]here should be no disagreement . . . that the criminal justice system does retain an important place in the ongoing effort to deter and punish terrorist acts without the sacrifice of American constitutional norms and bedrock values."²¹⁰ Even—if not especially—in such dangerous times, it is the duty of our civilian courts "calmly to poise the scales of justice, unmoved by the arm of power, undisturbed by the clamor of the multitude."²¹¹

209. *United States v. Rabinowitz*, 339 U.S. 56, 69 (1950) (Frankfurter, J., dissenting).

210. *Abu Ali*, 528 F.3d at 221.

211. *United States v. Bollman*, 24 F. Cas. 1189, 1192 (C.C.D.C. 1807) (No. 14,622).

Cyber Warfare and Precautions Against the Effects of Attacks

Eric Talbot Jensen *

Ninety-eight percent of all U.S. government communications travel over civilian-owned-and-operated networks. Additionally, the government relies almost completely on civilian providers for computer software and hardware products, services, and maintenance. This near-complete intermixing of civilian and military computer infrastructure makes many of those civilian objects and providers legitimate targets under the law of armed conflict. Other civilian networks, services, and communications may suffer collateral damage from legitimate attacks on government targets. To protect those civilian objects and providers from the effects of attacks, the law of armed conflict requires a state to segregate its military assets from the civilian population and civilian objects to the maximum extent feasible. Where segregation is not feasible, the government must protect the civilian entities and communications from the effects of attacks. The current integration of U.S. government assets with civilian systems makes segregation impossible and therefore creates a responsibility for the United States to protect those civilian networks, services, and communications. The U.S. government is already taking some steps in that direction, as illustrated by a number of plans and policies initiated over the past decade. However, the current actions do not go far enough. This Article identifies six vital actions the government must take to comply with the law of armed conflict and to ensure not only the survivability of military communication capabilities during times of armed conflict, but also the protection of the civilian populace and civilian objects.

I.	Introduction.....	1522
II.	Cyber “Attacks”	1524
III.	Interconnectivity, Targeting, and Feasibility Under Article 58(a) and (b)	1530
IV.	Alternative Responsibilities Under Article 58(c).....	1540
V.	U.S. Practice in Protecting Civilians and Civilian Cyber Objects.....	1543
VI.	Recommendations	1551
VII.	Conclusion	1556

* Visiting Assistant Professor, Fordham Law School. Previously Chief, International Law Branch, Office of The Judge Advocate General, U.S. Army; Military Legal Advisor to U.S. forces in Baghdad, Iraq and in Tuzla, Bosnia; Legal Advisor to the U.S. contingent of U.N. forces in Macedonia. Thanks to Sean Watts for his comments on an earlier draft and SueAnn Johnson for her invaluable research assistance.

I. Introduction

From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy, and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.

—President Barack Obama¹

In a recent address to open the 2010 Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology, former Director of National Intelligence Admiral Michael McConnell estimated that 98% of U.S. government communications, including classified communications, travel over civilian-owned-and-operated networks and systems.² The U.S. government does not control or protect these networks. The lack of effective security and protection of these and most other civilian computer networks led Admiral McConnell to predict that the United States will suffer an “electronic Pearl Harbor.”³ He further predicted that at some point the U.S. government is going to have to “reinvent” itself to better incorporate and account for advancing cyber technology.⁴ Finally, he predicted that the Internet is going to have to move from “dot com” to “dot secure.”⁵ Coming from his prior position,⁶ these remarks should cause those who read them to pause and wonder at the inevitability of these predictions.

In fact, the United States and other governments are very aware of the problem and are making efforts to combat their vulnerabilities.⁷ However,

1. Barack Obama, U.S. President, Remarks on Securing Our Nation’s Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure; see also Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 123 (2009) (quoting NATO’s Chief of Cyber Defense as stating that “cyber terrorism [and] cyber attacks pose as great a threat to national security as a missile attack”).

2. Michael McConnell, Former Dir. of Nat’l Intelligence, Keynote Address at the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology (Feb. 4, 2010). The Symposium was sponsored by the Texas Law Review in partnership with the Strauss Center for International Security and Law.

3. *Id.* Others have similarly predicted an electronic Pearl Harbor. See *Bush’s War Room: Richard Clarke*, ABC NEWS, Sept. 30, 2004, <http://abcnews.go.com/Politics/story?id=121056&page=1> (indicating that former Special Adviser for Cyberspace Security Richard Clarke became well-known for using the phrase “electronic Pearl Harbor”).

4. McConnell, *supra* note 2.

5. *Id.* The reference here is presumably to a move to an Internet architecture that provides a much more secure platform than the current system.

6. See Shane Harris, *The Cyberwar Plan*, NAT’L J., Nov. 14, 2009, available at http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (describing how McConnell “established the first information warfare center at the NSA in the mid-1990s”).

7. See *infra* notes 36–46 and accompanying text.

many of the current efforts do not go far enough in addressing these vulnerabilities. The efforts also do not fully respond to legal requirements under the law of war. One example of this shortcoming in current government action, and the topic of this Article, is the lack of preparedness to comply with the law-of-armed-conflict requirement to protect civilians and civilian objects from the effects of attacks. The law of war requires states to either segregate their military assets from civilians and civilian objects, or where segregation is not feasible, to protect those civilians and civilian objects.⁸ The pervasive intermixing of U.S. Department of Defense (DOD) networks with civilian networks,⁹ the vast percentage of DOD communications that travel over civilian lines of communication,¹⁰ the near-complete reliance on commercially produced civilian hardware and software for DOD computer systems,¹¹ and the reliance on civilian companies for support and maintenance of U.S. government computer systems¹² make segregation of military and civilian objects during an armed attack unfeasible. This interconnectedness also makes these civilian companies, networks, and lines of communication legitimate targets to an enemy during armed conflict. Therefore, the United States and other similarly situated countries have a duty to protect the civilian networks and infrastructure, and key civilian companies, from the effects of potential attacks.

Part II of this Article will briefly document the current state of cyber affairs with a focus on the pervasiveness of cyber “attacks.” This Part will also briefly highlight the complicating problem of the inability to attribute attacks in cyberspace. Part III will discuss the significance of the interconnectivity of DOD cyber capabilities with civilian networks and systems, including potential enemy-targeting decisions. The Part will go on to establish that, at this point, it is not feasible for the United States to segregate its cyber operations from civilian objects and infrastructure as required by Article 58,

8. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 58, *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 3 [hereinafter API].

9. McConnell, *supra* note 2.

10. *Id.*

11. See ROBERT H. ANDERSON & RICHARD O. HUNDLEY, RAND CORP., THE IMPLICATIONS OF COTS VULNERABILITIES FOR THE DOD AND CRITICAL U.S. INFRASTRUCTURES: WHAT CAN/SHOULD THE DOD DO? 1 (1998), <http://www.rand.org/pubs/papers/2009/P8031.pdf> (“Critical systems on which the security and safety of the United States depend are increasingly based on commercial off-the-shelf (COTS) software systems.”); cf. ENTERPRISE SOFTWARE INITIATIVE, DEP’T OF DEF., ESI OVERVIEW & HISTORY (2009), <http://www.esi.mil/LandingZone.aspx?id=101&zid=1> (explaining the DOD’s ESI mission to reduce the cost of commercial software and hardware, which the DOD is relying on “more than ever to run the business of the DoD”).

12. See, e.g., Press Release, IBM, IBM Awarded National Security Agency High Assurance Platform (HAP) Contract to Improve Secure Information Sharing (Feb. 7, 2008), <http://www-03.ibm.com/press/us/en/pressrelease/23460.wss> (explaining the NSA’s High Assurance Platform (HAP) program, in which the NSA works with privacy companies, like IBM, to develop next-generation computers and networking technology).

paragraphs (a) and (b), of Additional Protocol I to the 1949 Geneva Conventions (API).¹³ Part IV will analyze the alternative requirement of paragraph (c) of Article 58, which requires states that are unwilling or unable to segregate their military and civilian objects to protect the endangered civilians and civilian objects under their control from the effects of potential attack.¹⁴ Part V will review specific steps already taken by the United States in an attempt to protect civilian infrastructure and systems. Part VI will advocate further measures that should be taken to not only ensure compliance with Article 58, but to also better meet the stated goals of protecting the U.S. cyber networks and infrastructure.

II. Cyber “Attacks”

The recent attack¹⁵ on the massive search engine Google¹⁶ is indicative of the pervasive nature of the threat that exists in cyberspace. A recent report claimed that at least thirty other companies were subjects of the same attack,¹⁷ and it was further discovered that “[m]ore than 75,000 computer systems at nearly 2,500 companies in the United States and around the world ha[d] been hacked in what appear[ed] to be one of the largest and most sophisticated attacks by cyber criminals to date.”¹⁸ Experts assert that “thousands of companies” are currently compromised by cyber invasions.¹⁹ In many of these cases, the companies do not even know they are compromised until law enforcement authorities tell them.²⁰ By that time, they have already been victimized.

These attacks are not only pervasive, but also cheap to execute and expensive to detect, defend, and remediate.²¹ As President Obama noted in

13. API, *supra* note 8, art. 58.

14. *See id.* (mandating that the parties to a conflict take all necessary precautions to protect civilians and their objects from dangers resulting from military operations).

15. *See* NAT’L RESEARCH COUNCIL OF THE NAT’L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1–2 (William A. Owens et al. eds., 2009) (describing the nature of cyber attack and its potential use); Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT’L L. 391, 399–405 (2010) (detailing the anatomy of a cyber attack); Paul A. Walker, Rethinking Computer Network “Attack” (Dec. 31, 2009) (unpublished manuscript), available at http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=paul_walker (discussing what amounts to an “attack” with computer-network operations).

16. Ellen Nakashima et al., *Google Threatens to Leave China*, WASH. POST, Jan. 13, 2010, at A1.

17. Ellen Nakashima, *Google to Enlist NSA to Ward off Attacks*, WASH. POST, Feb. 4, 2010, at A1.

18. Ellen Nakashima, *Large Worldwide Cyber Attack Is Uncovered*, WASH. POST, Feb. 18, 2010, at A3.

19. Kim Zetter, *Report Details Hacks Targeting Google, Others*, WIRED, Feb. 3, 2010, <http://www.wired.com/threatlevel/2010/02/apt-hacks/>.

20. *Id.*

21. *See* Siobhan Gorman et al., *Insurgents Hack U.S. Drones*, WALL ST. J., Dec. 17, 2009, available at <http://online.wsj.com/article/SB126102247889095011.html>; PAUL ROSENZWEIG, AM.

his speech quoted at the beginning of this Article, “America’s economic prosperity in the 21st century will depend on cybersecurity.”²² According to Ty Sagalow, Chairman of the Internet Security Alliance Board of Directors, “An estimated \$1 trillion was lost in the United States in 2008 through cyber attacks.”²³ The cost of downtime alone from major attacks to critical national infrastructure “exceeds . . . \$6 million per day.”²⁴ And the frequency and cost of cyber attacks are increasing.²⁵

A recent report published by the Center for Strategic and International Studies (CSIS) and McAfee, Inc. surveyed 600 security and IT executives from critical infrastructure in fourteen countries and detailed their anonymous responses about their “practices, attitudes and policies on security—the impact of regulation, their relationship with government, specific security measures employed on their networks, and the kinds of attacks they face.”²⁶ Their responses portray a state of continual attack on critical national infrastructure by high-level and technologically capable adversaries.²⁷ One of the most telling statistics gathered from this survey was that the United States was perceived as “one of the three countries ‘most vulnerable to critical infrastructure cyberattack . . .’”²⁸ For all countries, but particularly for the United States, this is a problem that has the potential to dramatically affect civil life.²⁹

BAR. ASS’N STANDING COMM. ON LAW & NAT’L SEC., NATIONAL SECURITY THREATS IN CYBERSPACE 1–3 (2009), http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf (arguing that the unique features of cyberspace generally make traditional risk management ineffective and, even when possible, impractical because of the significant costs necessary for implementation).

22. Obama, *supra* note 1.

23. William Matthews, *Cyberspace May Be Locale of Next War, Group Warns*, FED. TIMES, Dec. 7, 2009, available at 2009 WLNR 25655353.

24. STEWART BAKER ET AL., CTR. FOR STRATEGIC & INT’L STUDIES, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 3 (2010), <http://csis.org/event/crossfire-critical-infrastructure-age-cyber-war>.

25. *Id.* at 5.

26. *Id.* at 1, 41 n.1.

27. *Id.* at 3–11; see also Mark Clayton, *US Oil Industry Hit by Cyberattacks: Was China Involved?*, CHRISTIAN SCI. MONITOR, Jan. 25, 2010, <http://www.csmonitor.com/layout/set/print/content/view/print/275786> (describing recent cyber attacks on major U.S. oil companies that “may have originated in China and that experts say highlight a new level of sophistication in the growing global war of Internet espionage”).

28. BAKER ET AL., *supra* note 24, at 30; see also Ellen Messmer, *DDoS Attacks, Network Hacks Rampant in Oil and Gas Industry, Other Infrastructure Sectors*, NETWORKWORLD, Jan. 28, 2010, <http://www.networkworld.com/news/2010/012710-ddos-oil-gas.html?page=1> (reviewing various statistics generated in the CSIS survey, including one listing the United States as one of the three countries perceived as most vulnerable to cyber attack).

29. See Matthews, *supra* note 23 (“By targeting the systems that control [U.S.] manufacturing plants, power generators, refineries and other infrastructure, attackers may be able to take control of—and even crash—power, water, traffic control and other critical systems . . .”); BAKER ET AL., *supra* note 24, at 30 (“Some experts suggested that the U.S. was seen as more vulnerable because it was more advanced—and more reliant than almost any other nation on computer networks.”).

The attacks on Google and others also highlight another significant problem that plagues cybersecurity, or at least responses to cyber invasions—the inability to attribute cyber attacks.³⁰ Attribution is the ability to know who is actually conducting the attacks. As one former U.S. law enforcement official stated, “Even if you can trace something back to a [computer], that doesn’t tell you who was sitting behind it.”³¹ This lack of ability to attribute an attack gives attackers “plausible deniability.”³² While “most owners and operators [of critical national infrastructure] believe that foreign governments are already engaged in attacks on critical infrastructure in their country,”³³ there is no way to positively establish that.³⁴ For example, one computer-security expert claims that “the majority of the data that gets exfiltrated [from the United States] ultimately finds its way to IP addresses in China, and that’s pretty much all anybody knows.”³⁵

The commercial world is not the only target of cyber attack. Indeed, “politically-motivated attacks are becoming more frequent and sustained.”³⁶ In its 2009 Virtual Criminology Report, McAfee, Inc. noted that there has been an increase in politically motivated cyber attacks, including attacks against the White House, Department of Homeland Security (DHS), U.S. Secret Service, and DOD.³⁷ A recent report stated that in 2007,

[T]he Departments of Defense, State, Homeland Security, and Commerce; NASA; and National Defense University all suffered major intrusions by unknown foreign entities. The unclassified e-mail of the secretary of defense was hacked, and DOD officials told us that the department’s computers are probed hundreds of thousands of times each day. A senior official at the Department of State told us the department had lost “terabytes” of information. Homeland Security

30. Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 A.F. L. REV. 1, 31 (2009).

31. BAKER ET AL., *supra* note 24, at 6.

32. *Id.* at 1; see also *Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace: Hearing Before the Subcomm. on Terrorism and Homeland Security of the S. Comm. on the Judiciary*, 111th Cong. (2009) (statement of Larry M. Wortzel, Vice Chairman, U.S.–China Economic and Security Review Commission), available at http://judiciary.senate.gov/hearings/testimony.cfm?id=4169&wit_id=8316 (emphasizing that one of the most important objectives in preparing for future cyber attacks should be “developing reliable attribution techniques to determine the origin of computer exploitations and attacks”).

33. BAKER ET AL., *supra* note 24, at 3.

34. See *The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade: Hearing Before the H. Comm. on Foreign Affairs*, 111th Cong. (2010) (statement of Larry M. Wortzel, Comm’r, U.S.–China Economic and Security Review Commission), available at <http://www.internationalrelations.house.gov/111/wor031010.pdf> (arguing that “even if the attacks can be traced to China, it is not clear who ordered the attacks”).

35. Zetter, *supra* note 19 (quoting Kevin Mandia, president–CEO of Mandiant, a computer-security firm).

36. Jeffrey Carr, *Under Attack from Invisible Enemies*, INDEP. (U.K.), Jan. 20, 2010, available at 2010 WLNR 1165835.

37. Press Release, McAfee, Inc., McAfee Inc. Warns of Countries Arming for Cyberwarfare (Nov. 17, 2009), http://newsroom.mcafee.com/article_display.cfm?article_id=3594.

suffered break-ins in several of its divisions, including the Transportation Security Agency. The Department of Commerce was forced to take the Bureau of Industry and Security off-line for several months, and NASA has had to impose e-mail restrictions before shuttle launches and allegedly has seen designs for new launchers compromised.³⁸

U.S. government computers and networks are constantly being probed,³⁹ and protection is a formidable task. In any twenty-four-hour period, DOD computers access the Internet “over one billion times.”⁴⁰ The DOD “operates 15,000 networks across 4,000 installations in 88 countries. [They] use more than 7 million computer devices. It takes 90,000 personnel and billions of dollars annually to administer, monitor and defend those networks.”⁴¹ DHS recently received funding to hire up to one thousand cybersecurity experts to help “the nation’s defenses against cyberthreats,”⁴² and DOD “ordered all troops and officials involved in protecting computer networks from enemy hackers to undergo training in computer hacking” under the premise that “to beat a hacker, you must think like one.”⁴³ At a recent Senate subcommittee hearing, Senator Thomas R. Carper stated that in the last year “federal agencies have spent more on cyber security than the entire Gross Domestic Product of North Korea.”⁴⁴ It is estimated that “more than 100 foreign intelligence organizations are trying to break into U.S. systems”⁴⁵ and known cyber attacks against U.S. computers rose to 37,258 in 2008 from 4,095 in 2005.⁴⁶ Terrorist organizations such as al Qaeda are transitioning many of

38. COMM’N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, CTR. FOR STRATEGIC & INT’L STUDIES, *SECURING CYBERSPACE FOR THE 44TH PRESIDENCY* 12–13 (2008), http://csis.org/files/media/isis/pubs/081208_securingcyberspace_44.pdf.

39. See Schapp, *supra* note 1, at 141–42 (providing two examples of recent incidents in which hackers penetrated U.S. government computer systems).

40. Joshua E. Kastenberg, *Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DOD to Take Time-Sensitive Action on the NIPRNET*, 64 A.F. L. REV. 175, 183 (2009).

41. William J. Lynn III, Deputy Sec’y of Def., Remarks at the USAF–TUFTS Institute for Foreign Policy Analysis Conference (Jan. 21, 2010), <http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1410>.

42. Carol Cratty, *DHS to Hire up to 1,000 Cybersecurity Experts*, CNN POLITICS.COM, Oct. 2, 2009, <http://www.cnn.com/2009/POLITICS/10/02/dhs.cybersecurity.jobs/index.html> (quoting Secretary of Homeland Security Janet Napolitano).

43. Bill Gertz, *Inside the Ring*, WASH. TIMES, Mar. 4, 2010, at A8.

44. *More Security, Less Waste: What Makes Sense for Our Federal Cyber Defense: Hearing Before the Subcomm. on Fed. Financial Management, Government Information, Fed. Servs., and International Security of the S. Comm. on Homeland Security and Governmental Affairs*, 111th Cong. (2009) (statement of Sen. Thomas R. Carper, Chairman, Subcomm. on Fed. Financial Management, Government Information, Fed. Servs., and International Security), available at http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=8505fb0f-bf9b-4bb4-9e25-e71154391202.

45. Lynn, *supra* note 41.

46. Siobhan Gorman, *Bush Looks to Beef Up Protection Against Cyberattacks*, WALL ST. J., Jan. 28, 2008, at A9.

their efforts to the Internet,⁴⁷ causing FBI Director Robert S. Mueller to state that “Al-Qaeda’s online presence has become as potent as its physical presence.”⁴⁸

Attacks are not focused solely on the United States. Countries such as Tatarstan, Kyrgyzstan, Iran, Zimbabwe, Israel, and South Korea have been the targets of attacks within the last two years.⁴⁹ Additionally, there are the famous cases of Estonia in 2007⁵⁰ and Georgia in 2008⁵¹ where cyber attacks severely degraded the government’s ability to govern. The attacks in Estonia targeted not only government Web sites but also included many of the country’s banks and other civilian infrastructure.⁵² Even more telling for the topic of this Article, “[h]ackers mounted coordinated assaults on Georgian government, media, banking and transportation sites in the weeks before Russian troops invaded.”⁵³ These recent historical examples show not only the propensity to attack governments but also the natural integration of cyber attacks with future kinetic attacks. This is almost certainly a trend that will increase.⁵⁴ As demonstrated by the attacks on Georgia and Estonia,

47. See Toby Harnden, *Al-Qa’eda Plans Cyber Attacks on Dams*, DAILY TELEGRAPH, June 28, 2002, <http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1398683/Al-Qaeda-plans-cyber-attacks-on-dams.html> (“Al-Qa’eda have been investigating how to carry out devastating attacks through cyberspace by seizing control of dam gates or power grids using the internet.”); Pauline Neville-Jones, *Statement on Governments and Cyber Warfare* (Mar. 11, 2010), http://www.conservatives.com/News/Speeches/2010/03/Pauline_Neville-Jones_Governments_and_Cyber_Warfare.aspx (noting that terrorists rely on the Internet for recruiting and planning purposes).

48. Ellen Nakashima, *FBI Director Warns of ‘Rapidly Expanding’ Cyberterrorism Threat*, WASH. POST, Mar. 4, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html>.

49. Carr, *supra* note 36.

50. Anne Applebaum, *For Estonia and NATO, a New Kind of War*, WASH. POST, May 22, 2007, at A15; Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at A1; *US Warns Cyber-Attacks Will Increase*, FIN. TIMES, May 18, 2007, at 12; Toomas Hendrik Ilves, President, Republic of Estonia, Remarks at the International Cyber Conflict Legal and Policy Conference in Tallinn (Sept. 9, 2009), http://www.president.ee/en/media/press_releases.php?gid=130312. The attacks on Estonia prompted NATO to fund and create a new research center designed to boost their cooperative defenses against cyber attacks. *Cyberterrorism Defense*, WASH. POST, May 14, 2008, at A13.

51. James R. Asker, *Cyber Zap*, AVIATION WK. & SPACE TECH., Sept. 7, 2009, at 24; Siobhan Gorman, *Cyberwarfare Accompanies the Shooting*, WALL ST. J., Aug. 12, 2008, at A9.

52. BAKER ET AL., *supra* note 24, at 17.

53. Brandon Griggs, *U.S. at Risk of Cyberattacks, Experts Say*, CNN, Aug. 18, 2008, <http://www.cnn.com/2008/TECH/08/18/cyber.warfare/index.html>; see also Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 4–5 (2009) (“In July 2008, shortly before armed conflict broke out between Russia and Georgia, hackers barraged Georgia’s Internet infrastructure with coordinated cyberattacks. The attacks overloaded and shut down many of Georgia’s computer servers, and impaired Georgia’s ability to disseminate information to its citizens during its armed conflict with Russia.”).

54. See Jaak Aaviksoo, Minister of Defense, Republic of Estonia, *Strategic Impact of Cyber Attacks*, Address at the Royal College of Defense Studies (May 3, 2010), <http://www.irl.ee/en/Media/Articles/1927/strategic-impact-of-cyber-attacks> (discussing the threat of

attribution continues to be a problem in the case of attacks against state-computer systems.⁵⁵ Without the ability to attribute, it is difficult to equate these attacks to acts of armed conflict.⁵⁶

It is clear that states, in conjunction with upgrading their cyber defenses, are also developing cyber-offensive capability.⁵⁷ As mentioned previously,⁵⁸ many of the IT and security professionals who responded to the CSIS survey believed that foreign governments were behind at least some of the attacks on their networks.⁵⁹ The United Nations has collected statements by a number of nations concerning their views on cyberspace,⁶⁰ but few clear answers have emerged.

“coordinated cyber attacks towards [a] country’s critical information infrastructure . . . organized together with physical attacks”).

55. See Schaap, *supra* note 1, at 144–46 (recounting the cyber attacks that were mounted against Estonian and Georgian computer systems and noting that “there is no conclusive proof of who was behind the attacks”); Watts, *supra* note 15, at 397–98 (elaborating on the difficulty of identifying the “precise source” of the Russian attacks on Georgian and Estonian computer networks).

56. See Sklerov, *supra* note 53, at 6–10 (explaining that “because the law of war forbids states from responding with force unless an attack can be attributed to a foreign state or its agents,” the attribution problem forces governments to treat cyber attacks as criminal matters rather than as traditional armed assaults).

57. BAKER ET AL., *supra* note 24, at 5 (“In 2007, McAfee’s annual Virtual Criminology Report concluded that 120 countries had, or were developing, cyber espionage or cyber war capabilities.”); see also RAY WALSER, HERITAGE FOUND., STATE SPONSORS OF TERRORISM: TIME TO ADD VENEZUELA TO THE LIST (2010), <http://www.heritage.org/Research/Reports/2010/01/State-Sponsors-of-Terrorism-Time-to-Add-Venezuela-to-the-List> (warning of Cuba’s developing capacity for cyber warfare, aided by the Russians and Chinese).

58. See *supra* notes 26–27 and accompanying text.

59. BAKER ET AL., *supra* note 24, at 3.

60. See The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–13, delivered to the General Assembly, U.N. Doc. A/64/129/Add.1 (Sept. 9, 2009); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–17, delivered to the General Assembly, U.N. Doc. A/64/129 (July 8, 2009); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–8, delivered to the General Assembly, U.N. Doc. A/63/139 (July 18, 2008); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 1–3, delivered to the General Assembly, U.N. Doc. A/62/98/Add.1 (Sept. 17, 2007); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–14, delivered to the General Assembly, U.N. Doc. A/62/98 (July 2, 2007); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–8, delivered to the General Assembly, U.N. Doc. A/61/161 (July 18, 2006); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 3, delivered to the General Assembly, U.N. Doc. A/60/95 (July 5, 2005); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–13, delivered to the General Assembly, U.N. Doc. A/59/116 (June 23, 2004); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–17, delivered to the General

The ubiquity of cyber attack cannot be questioned. However, each state's response to the problem is certainly an open question. While issues of attribution complicate a state's response, every state has to be prepared to protect itself and its citizens from the consequences of cyber attack. It is on this issue that this Article focuses next.

III. Interconnectivity, Targeting, and Feasibility Under Article 58(a) and (b)

As mentioned in the introduction to this Article, 98% of U.S. government communications travel over civilian-owned-and-operated networks.⁶¹ This includes both unclassified and classified messaging and would presumably include communications that are military orders and directions for conducting military operations. It would likely also include current intelligence and information reports coming from the battlefield to update strategic decision makers in the Pentagon and other headquarters.⁶²

These communications are military objectives and would be targetable by an enemy during armed conflict. The definition of military objectives is contained in Article 52 of the API.⁶³ Article 52 is titled "General protection

Assembly, U.N. Doc. A/58/373 (Sept. 17, 2003); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 1-3, delivered to the General Assembly, U.N. Doc. A/57/166 (July 2, 2002); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2-6, delivered to the General Assembly, U.N. Doc. A/56/164/Add.1 (Oct. 3, 2001); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2-5, delivered to the General Assembly, U.N. Doc. A/56/164 (July 3, 2001); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2-7, delivered to the General Assembly, U.N. Doc. A/55/140 (July 10, 2000); The Secretary-General, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2-13, delivered to the General Assembly, U.N. Doc. A/54/213 (Aug. 10, 1999) (reporting responses from various countries expressing their appreciation of information-security issues and ideas about measures to strengthen information security in the future); see also The Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2, delivered to the General Assembly, U.N. Doc. A/60/202 (Aug. 5, 2005) (reporting on the communications between the governmental experts on information security); Sean Kanuck, Int'l Att'y and Senior Intelligence Analyst, *Sovereign Discourse on Cyber Conflict Under International Law*, Remarks at the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology (Feb. 6, 2010), *audio available at* <http://www.texasrev.com/symposium/listen> (discussing various countries' responses to U.N. requests and the current group of governmental experts on information security).

61. See *supra* note 2 and accompanying text.

62. See Howard S. Dakoff, Note, *The Clipper Chip Proposal: Deciphering the Unfounded Fears That Are Wrongfully Derailing Its Implementation*, 29 J. MARSHALL L. REV. 475, 479 (1996) (noting that the types of military communications transmitted over private networks "include the designing of weapons, the guiding of missiles, the managing of medical supplies, the mobilization of reservists and the relaying of battle tactics to combat commanders").

63. API, *supra* note 8, art. 52 ("[M]ilitary objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization . . . offers a distinct military advantage.").

of civilian objects” and clarifies that civilian objects are not targetable.⁶⁴ It also contrasts civilian objects with military objectives.⁶⁵

A. government’s military or intelligence-agency⁶⁶ computers, routers, networks,⁶⁷ cables, and other cyber assets are targetable because of their use facilitating military communications. If these objects were performing the same functions for a civilian company, rather than the government, they would be protected from attack as civilian objects. It is their use by the military or intelligence agencies that makes them targetable.⁶⁸ Though it concerned radio and television instead of cyber communication, this is apparently the analysis that NATO leaders applied before bombing a radio and television station in Belgrade during the Kosovo air campaign in 1999.⁶⁹ Such an action, though protested by Serbia, was not found to be unlawful.⁷⁰

Similarly, the government procures the vast majority of its hardware and software from commercial suppliers. Much of this software and hardware is also maintained by civilian companies.⁷¹ These companies that manufacture and service government hardware and software may be targetable. In the event of a sustained attack against the United States’ cyber capabilities, these civilian companies would likely be contacted for support and maintenance.⁷² Further, the U.S. government is the “single largest

64. *Id.*

65. *See id.* (“Civilian objects are all objects which are not military objectives as defined in paragraph 2.”).

66. There may be other government computers, routers, networks, cables, and other assets that would also be targetable based on their use.

67. *But see* Joshua E. Kastenberg, *Non-intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43, 55 (2009) (recognizing a memorandum from the U.S. Air Force Operations and International Law division as taking the position that a network does not constitute a weapons system). This may affect an attacker’s analysis as to whether a network is targetable by its nature as opposed to its use.

68. *See* API, *supra* note 8, art. 52 (“[M]ilitary objectives are . . . those objects which by their . . . use make an effective contribution to military action . . .” (emphasis added)).

69. Justin Brown & Phil Miller, *Foreign Journalists Feel the Heat of Backlash*, SCOTSMAN, Apr. 24, 1999, available at http://findarticles.com/p/articles/mi_7951/is_1999_April_24/ai_n32632439/?tag=content; Paul Richter, *Milosevic Not Home as NATO Bombs One of His Residences*, L.A. TIMES, Apr. 23, 1999, at A34.

70. *See* Int’l Criminal Tribunal for the Former Yugo., June 13, 2000, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia*, ¶ 72, 39 I.L.M. 1257, 1283 (noting NATO’s stress of the civil television network’s “dual-use”).

71. *See, e.g.*, Press Release, Lockheed Martin, Lockheed Martin Awarded \$5.8M Contract to Maintain Pentagon Electronic Messaging Systems (Aug. 20, 2008), http://www.lockheedmartin.com/news/press_releases/2008/0820_pentagon-netcents-contract.html (reporting the selection of Lockheed Martin, a civilian company, “to operate and maintain the message routing infrastructure for the Pentagon’s command messaging systems”).

72. Civilians who work at these companies would be targetable to the extent that they take a “direct part in hostilities.” *See* API, *supra* note 8, art. 51 (“Civilians shall enjoy the protection afforded by this section, unless and for such time as they take a direct part in the hostilities.”). The meaning of this term is highly contested and beyond the scope of this Article. *See generally* NILS MELZER, INT’L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT

purchaser of information security products.”⁷³ These security products are purchased from civilian suppliers who presumably will supply security updates and assistance to maintain the security of government systems. This reliance on civilian cyber companies to maintain government cyber systems and update cyber products brings the premises and objects used by these civilian companies potentially within the targeting options of an attacking enemy as well. If a civilian computer company produces, maintains, or supports government cyber systems, it seems clear that an enemy could determine that company meets the test of Article 52 and is targetable.

Discrete electronic-military communications, such as an e-mail transmitting an attack order or delivering an intelligence report, are also targetable by their nature. Targeting and interrupting these communications would obviously be of great benefit to an enemy during an armed conflict. As will be discussed below, targeting specific electronic communications presents technological difficulties, but under the law, it is clear that these discrete communications are targetable.⁷⁴

Each of the military targets just listed is likely to be intermixed with civilian objects in the interconnected cyber world.⁷⁵ The surrounding civilian objects cannot be directly attacked. But the company that manufactures government computers or routers will likely also manufacture them for sale to civilians.⁷⁶ The software company that provides a “help desk” for government assistance will likely also have employees who work in the same area answering questions for civilians.⁷⁷ The company that produces security software and sends out “patches” to cover vulnerabilities will likely produce and send those patches to both government and civilians.⁷⁸ And fiber-optic

PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 41–68 (2009) (attempting to interpret “direct participation in hostilities” in a useful way with little guidance from the primary sources); Watts, *supra* note 15, at 392 (discussing the inadequacy of current law-of-war status determinations).

73. Daniel M. White, *The Federal Information Security Management Act of 2002: A Potemkin Village*, 79 *FORDHAM L. REV.* (forthcoming 2010).

74. See *supra* notes 63–65 and accompanying text.

75. See Harris, *supra* note 6 (noting that, in 2003, the United States decided against attacking Iraq’s military communications networks with a cyber attack because of intermixing with civilian systems).

76. Civilian objects that serve both civilian and military purposes are often termed “dual-use.” Jeanne M. Meyer, *Tearing Down the Facade: A Critical Look at the Current Law on Targeting the Will of the Enemy and Air Force Doctrine*, 51 *A.F. L. REV.* 143, 178 (2009). This term is somewhat misleading because at the point the civilian business or object serves a military purpose, it becomes a military object. The portions of that object that continue to provide services to civilians do not change the target back to a civilian object. Rather, they require the commander ordering the attack to consider that in his proportionality analysis discussed below.

77. See, e.g., Microsoft Government, Contact Us, <http://www.microsoft.com/industry/government/products/contactus.mspix> (providing government users with contact information for support regarding Microsoft software).

78. See, e.g., Microsoft Government, Microsoft Infrastructure Optimization Model, <http://www.microsoft.com/industry/government/solutions/itinrastructureoptimization.mspix> (describing Microsoft services able to patch operating systems and desktops).

wires that carry military communications will also carry civilian communications. The portions of these companies or services that support the government may be legitimate targets under the law of war, while the portions that do not are protected from direct attack.⁷⁹ The civilian portions are not, however, preserved from the effects of attacks on legitimate military objectives. The case of a fiber-optic communication line is illustrative.

With 98% of day-to-day government communications routinely traveling over civilian communication lines, there will be many civilian lines of communication that will carry targetable electronic traffic intermixed with civilian traffic. Those specific military communications are still targetable, but the networks and lines would not be. However, because of the nature of electronic communications, it is very difficult to target a single communication once it is in transit.⁸⁰ The attacker may still be able to attack the military objective, such as the individual military communication, but he would have to determine that he could actually destroy or degrade the military communication and then weigh the military benefit of destroying that military communication against the incidental destruction to civilian networks and communications and ensure the destruction was not excessive compared to the benefit the attacker would receive. This analysis is known as the principle of proportionality, and it is contained in Article 57.2(a)(iii) of API.⁸¹

Article 57. Precautions in attack

1. In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.
2. With respect to attacks, the following precautions shall be taken:
 - (a) those who plan or decide upon an attack shall:
 - (i) do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives within the meaning of paragraph 2 of Article 52 and that it is not prohibited by the provisions of this Protocol to attack them;
 - (ii) take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event

79. See API, *supra* note 8, art. 52(2) (stating that attacks shall be limited to military objectives).

80. See E. Judson Jennings, *Carnivore: U.S. Government Surveillance of Internet Transmissions*, 6 VA. J.L. & TECH. 10, ¶¶ 8–9 (2001), <http://www.vjolt.net/vol6/issue2/v6i2-a10-Jennings.html> (describing the FBI's Carnivore program, which is used to intercept targeted communications, and explaining how “[a] single communication is broken into many smaller packets” when in transit).

81. API, *supra* note 8, art. 57(2)(a)(iii); E. L. Gaston, *Mercenarism 2.0? The Rise of the Modern Private Security Industry and Its Implications for International Humanitarian Law Enforcement*, 49 HARV. INT’L L.J. 221, 244 (2008).

to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects;

(iii) refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated⁸²

It is clear that these two fundamental law-of-war targeting provisions of military objective and proportionality apply to cyber attacks conducted during armed conflict.⁸³ Attackers can only target cyber elements that are military objectives, and any attacks against military objectives must comply with the principle of proportionality. There are many nuances to the application of these principles that are beyond the scope of this Article and have been amply covered elsewhere.⁸⁴ It is sufficient to establish that a state's cyber activities are targetable by an enemy and are likely to be attacked in times of armed conflict. Further, network and system operators who have military communications traversing their computers and networks may be opening themselves up to attack by an enemy that has performed a proportionality analysis and determined that the benefit of destroying these civilian networks and systems is not excessive considering the degradation to the U.S. government communications that would be achieved.

In addition to prescribing who and what an attacker can attack, the law of war also puts an affirmative obligation on the defender with regard to civilians and civilian objects.⁸⁵ This affirmative obligation is known as "precautions against the effects of attacks" and requires the defender to take certain precautions to protect civilians and civilian objects from the potential dangers of anticipated attacks.⁸⁶ This obligation to protect civilians and civilian objects has its modern foundation in the 1863 Lieber Code, which stated that "[c]lassical works of art, libraries, scientific collections, or precious instruments, such as astronomical telescopes, as well as hospitals, must be

82. API, *supra* note 8, art. 57.

83. See Eric Talbot Jensen, *Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?*, 18 AM. U. INT'L L. REV. 1145, 1154-61 (2003) (reviewing the two-prong test that must be satisfied to overcome the preclusion against attacking civilian objects and issues related to its typical application and then applying those concepts to computer-networks attacks); Schaap, *supra* note 1, at 158 ("When analyzing the lawfulness of a cyber warfare operation one should conduct the same analysis as when determining the lawfulness of an aircraft targeting a military objective."). *But see* Watts, *supra* note 55, at 440-43, 446-47 (arguing that other principles of the law of war, such as the requirements for combat status, may need to be revised).

84. See Jensen, *supra* note 83, at 1154-61 (reviewing the requirements for attacking civilian objects where doing so serves military objectives and then applying those concepts to computer-networks attacks); Schaap, *supra* note 1, at 149-60 (analyzing the use of cyber-warfare operations in relation to the law of war).

85. API, *supra* note 8, art. 58.

86. *Id.*

secured against all avoidable injury, even when they are contained in fortified places whilst besieged or bombarded.”⁸⁷ While it is unclear from the text who had this responsibility, it presumably applied to whomever was in possession of the civilian objects, which would certainly have been the defender in many cases, such as in a siege or bombardment.

The affirmative obligation was clarified in the Annex to the 1907 Hague Convention IV.⁸⁸ In Article 27, it states that the besieged has the duty to indicate the presence of “buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected . . . by distinctive and visible signs, which shall be notified to the enemy beforehand.”⁸⁹ The same Article imposes a responsibility on the attacker to spare such marked buildings “provided they are not being used at the time for military purposes.”⁹⁰

This principle of a defender’s responsibility to protect civilians and civilian objects was revisited in the preparations for the 1977 conference that produced the Additional Protocols to the 1949 Geneva Conventions.⁹¹ The International Committee of the Red Cross (ICRC) proposed a text that became the basis for the conference’s negotiations.⁹² This draft contained a provision—originally Article 51, but it would eventually become Article 58—that concerned the defender’s responsibilities for its civilians and civilian objects. The obligation was basically set in the alternative: either

87. FRANCIS LIEBER, WAR DEP’T, INSTRUCTIONS FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD ¶ 35 (1863) [hereinafter LIEBER CODE], reprinted in 2 FRANCIS LIEBER, THE MISCELLANEOUS WRITINGS OF FRANCIS LIEBER: CONTRIBUTIONS TO POLITICAL SCIENCE 245, 254 (1881). Two other provisions allow for the protection of certain civilian objects but do not make it an affirmative obligation:

115. It is customary to designate by certain flags (usually yellow) the hospitals in places which are shelled, so that the besieging enemy may avoid firing on them. The same has been done in battles, when hospitals are situated within the field of the engagement.

.....

118. The besieging belligerent has sometimes requested the besieged to designate the buildings containing collections of works of art, scientific museums, astronomical observatories, or precious libraries, so that their destruction may be avoided as much as possible.

Id. at 267, 268.

88. Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land art. 27, Oct. 18, 1907, 1 Bevans 631 [hereinafter Hague IV].

89. *Id.*

90. *Id.*

91. 1 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE ON THE REAFFIRMATION AND DEVELOPMENT OF INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICTS, GENEVA (1974–1977), pt. 1, at 3 (1978) [hereinafter OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE].

92. *Id.*

protect the civilians under your control or segregate them from areas where they are endangered. The draft proposal initially stated:

Article 51. Precautions against the effects of attacks

1. The Parties to the conflict shall, to the maximum extent feasible, take the necessary precautions to protect the civilian population, individual civilians and civilian objects under their authority against the dangers resulting from military operations.
2. They shall endeavour to remove them from the proximity of military objectives, subject to Article 49 of the Fourth Convention, or to avoid that any military objectives be kept within or near densely populated areas.⁹³

Once the conference convened, the draft was sent to a working group where the discussion seemed to revolve around two key points: the practicability of the obligation and whether the obligation was *de facto* or *de jure*.⁹⁴ The representative from Canada, Brigadier General (BG) J.P. Wolfe, who was the Judge Advocate General for the Department of National Defense, proposed two changes that dealt with both of these concerns.⁹⁵ In the first proposal, BG Wolfe urged changing the language of paragraph one from “authority” to “control.” He argued that “use of the word ‘control’ would impose obligations on the parties which would not necessarily be implied by the use of the word ‘authority.’ It referred to the *de facto* as opposed to the *de jure* situation.”⁹⁶ It is clear from the negotiating record that this proposed amendment was viewed mostly in terms of geography, and that phenomena such as the Internet were not envisioned in the deliberations.⁹⁷ Therefore, control was thought of as a territorial term.⁹⁸ The proposed amendment was eventually accepted.⁹⁹

The second proposal by BG Wolfe was to have the limiting language, “to the maximum extent feasible,” apply generally to the Article, rather than to the first paragraph only.¹⁰⁰ His concern was reflected by several other delegations who were concerned that “countries would find it difficult to

93. *Id.* art. 51, at 17.

94. 14 *id.* at 198–99 (“[T]he use of the word ‘control’ would impose obligations on the parties which would not necessarily be implied by the use of the word ‘authority.’ It referred to the *de facto* as opposed to the *de jure* situation.”).

95. *Id.* at 198–99.

96. *Id.* at 198.

97. 1 *id.* pt. 1, art. 51, at 147; COMMENTARY TO THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 692 (Yves Sandoz et al. eds., 1987).

98. COMMENTARY TO THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, *supra* note 97, at 692. It is interesting to note here that the United States has recently begun to view cyberspace as a domain equal to air, land, and sea. See Ellen Nakashima, *Pentagon to Announce ‘Cyber Command,’* WASH. POST, June 13, 2009, at A5 (articulating the Pentagon’s “cyber-command” strategy).

99. API, *supra* note 8, art. 58.

100. 14 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE, *supra* note 91, at 199.

separate civilians and civilian objects from military objectives.”¹⁰¹ John Redvers Freeland, the United Kingdom head of delegation for the second, third, and fourth sessions, emphasized that protections such as those contemplated in Article 51 can “never be absolute” and that the words “to the maximum extent feasible” related to what was “workable or practicable, taking into account all the circumstances at a given moment, and especially those which had a bearing on the success of military operations.”¹⁰² This same idea was advocated by S.H. Bloembergen, a delegate from the Netherlands, who stated that “feasible” should be “interpreted as referring to that which was practicable or practically possible, taking into account all circumstances at the time.”¹⁰³

After modification in the working group to its present form, the Article was voted on and adopted by consensus¹⁰⁴ with George H. Aldrich, the head of the U.S. delegation, reporting that the modified text “had been the most generally acceptable”¹⁰⁵ to those involved in the negotiations. As amended and approved, the new Article 58 states:

The Parties to the conflict shall, to the maximum extent feasible:

- (a) Without prejudice to Article 49 of the Fourth Convention, endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives;
- (b) Avoid locating military objectives within or near densely populated areas;
- (c) Take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations.¹⁰⁶

Though modified and reordered, the two fundamental alternatives from the original Article 51 remain the gravamen of the Article: either protect the civilians under your control or segregate them from areas where they are endangered.¹⁰⁷ Reinforcing the understanding during the negotiations, many states added declarations upon signature of the API that these obligations were subject to the language, “maximum extent feasible,” and that such language required only that which was practicable, based on the conditions and situation prevailing at the time.¹⁰⁸

101. 15 *id.* at 353.

102. 6 *id.* at 214.

103. *Id.*

104. 14 *id.* at 304.

105. *Id.*

106. API, *supra* note 8, art. 58.

107. See *supra* note 93 and accompanying text.

108. See International Committee of the Red Cross, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, <http://www.icrc.org/ihl.nsf/WebSign?ReadForm&id=470&ps=P>

The United States is a signatory to the API but not a party because the Senate has never given its advice and consent.¹⁰⁹ However, in his seminal article on the United States' position concerning the API, Mike Matheson stated that the United States "support[ed] the principle" in Article 58.¹¹⁰ Additionally, not only is there no record of any statements by the U.S. government against Article 58, but the U.S. Navy's military manual states the principle as applicable to U.S. operations.¹¹¹ Further, in its recent Customary International Humanitarian Law Study, the ICRC lists precautions against the effects of attacks as customary international law,¹¹² binding on all states whether or not they are parties to the API.¹¹³ While there has been no official statement, there is also no indication that the United States would not accept the provisions of Article 58 as an affirmative obligation during armed conflict.

Accepting Article 58's obligation to segregate or protect, either as binding on the United States or as a principle the United States would accede to in armed conflict, the following example is typical of an application of Article 58 to a non-cyber armed-conflict situation. Assume the military determined that it needed to establish a military-supply depot at a normally civilian seaport. Because of the military's use of the seaport, that part used by the military would become a military objective under Article 52 and would

(listing the state parties and signatories to the API). In particular, the declarations of Algeria, Australia, Austria, Belgium, Canada, Ireland, Italy, the Netherlands, New Zealand, Spain, and the United Kingdom describe this "practicable" framework. *Id.* (follow "text" hyperlink for each).

109. See Theodor Meron, Editorial Comment, *The Time Has Come for the United States to Ratify Geneva Protocol I*, 88 AM. J. INT'L L. 678, 678–80 (1994) (describing President Regan's request that the Senate give its advice and consent to the ratification of Protocol II alone); International Committee of the Red Cross, *supra* note 108 (noting that a state becomes a party by signing and ratifying a treaty).

110. See Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. J. INT'L L. & POL'Y 419, 426–27 (1987) ("We support the principle that all practicable precautions, taking into account military and humanitarian considerations, be taken in the conduct of military operations to minimize incidental death, injury, and damage to civilians and civilian objects . . ."). *But see* Memorandum for John H. McNeill, Assistant Gen. Counsel (International), OSD (May 9, 1986), in LAW OF WAR DOCUMENTARY SUPPLEMENT 399–401 (Porter Harlow ed., 2008) (describing the portions of API that law-of-war experts thought were either part of customary international law or supportable for inclusion as customary international law through state practice, and noting that Article 58 was not listed in the memorandum).

111. See U.S. DEP'T OF THE NAVY, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS ¶ 8.3.2 (2007) ("A party to an armed conflict has an affirmative duty to remove civilians under its control (as well as the wounded, sick, shipwrecked, and prisoners of war) from the vicinity of objects of likely enemy attack.").

112. I JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 68–71 (2005). The study lists Rule 22 as, "The parties to the conflict must take all feasible precautions to protect the civilian population and civilian objects under their control against the effects of attacks." *Id.* at 68.

113. See Source: Custom, 1 HACKWORTH DIGEST § 3, at 15–17 (explaining that a rule of international law can develop from the practice of states if it has been of "sufficient duration and uniformity").

be targetable. If an enemy decided to attack the seaport, it would have to conduct a proportionality analysis under Article 57 based on the potential injury or death to civilians and damage to the civilian portions of the port area.¹¹⁴

Anticipating the potential for attack, under Article 58(a), the defending military would be obligated to the “maximum extent feasible” to “endeavour” to remove the civilians and civilian-shipping concerns from that portion of the seaport so if the enemy decided to attack the military portion of the port, that attack would put the fewest number of civilians and civilian objects at risk.¹¹⁵ Additionally, under Article 58(b), if the seaport was in the midst of a densely populated area, the military would have to try to situate its portions of the seaport as far away from the civilian population as feasible.¹¹⁶

Applying this analysis to cyber warfare illustrates the immediate difficulties inherent in the interconnectedness of U.S. government and civilian systems and the near-complete government reliance on civilian companies for the supply, support, and maintenance of its cyber capabilities. The U.S. government cannot, at this point, segregate its cyber capabilities from civilians and civilian objects. Given that 98% of the government’s communications go through civilian networks and systems over civilian lines,¹¹⁷ such segregation would require the government to establish its own lines of communication throughout the world,¹¹⁸ connecting its dispersed military installations.¹¹⁹ The government would also have to create its own computer hardware and software companies that could produce, support, and maintain state-of-the-art computer capabilities. Further, the government would have

114. API, *supra* note 8, art. 57.

115. *Id.*

116. *Id.*

117. *See supra* note 2 and accompanying text.

118. While the government is working on the “Global Information Grid,” a part of which would include secure computing and communications infrastructure, the current vision is only of a future system that is not within today’s technological capabilities. *See* U.S. DEP’T OF DEF., GLOBAL INFORMATION GRID ARCHITECTURAL VISION 1–6 (2007), available at <http://cio-nii.defense.gov/docs/GIGArchVision.pdf> (“The current GIG is characterized by organizational and functional stovepipe systems with varying degrees of interoperability and constrained access to needed information. It does not sufficiently exploit the potential of information age technologies, and does not fully support the operational imperative for the right information at the right time.”); Chris Paine, *U.S. Military to Install Global Internet Architecture Giving a “God-Like” View of Planet*, INFOWARS.COM, July 13, 2009, <http://www.infowars.com/u-s-military-to-install-global-internet-architecture-giving-a-god-like-view-of-planet/> (“The GIG, or Global Information Grid is a worldwide surveillance network that will give anyone linked into it instant information, at the users request, about anything, anytime, anywhere in the world!”); *cf. State’s Fibre Optic Cable Raises Cost, Benefits Questions*, STABROEK NEWS, Feb. 7, 2010, <http://www.stabroeknews.com/2010/stories/02/07/state%E2%80%99s-fibre-optic-cable-raises-cost-benefits-questions/print/> (analyzing Guyana’s plan to create a fiber-optic cable exclusively dedicated to e-governance).

119. *See* Lynn, *supra* note 41 (stating that the DOD currently uses 15,000 networks across 4,000 military installations in eighty-eight different countries).

to establish its own system of routers, switches, and telecom hotels to manage and protect these communications.

While these options may be conceivably “feasible,” they are not “practicable,” to use the words from Bloembergen during the negotiations.¹²⁰ Rather, the current practice of governments, and certainly the U.S. government, appears to embrace the interconnectedness with civilian systems, making segregation under Article 58(a) and (b) infeasible.¹²¹ Even understanding the risk associated with the interconnectedness of military and civilian cyber systems, governments have not taken affirmative steps to segregate military and civilian systems. If anything, the tendency is to move toward more interconnectivity.¹²² Segregation is not the preferred option for meeting obligations under Article 58 to protect civilians and civilian objects against the effects of attack.

But that must not be the end of the inquiry. It is certainly not in keeping with the spirit of the law of armed conflict for government action to bring civilians and civilian companies within the scope of lawful attacks and then to allow those same governments to leave the civilians and civilian companies completely alone to defend themselves. In fact, this is not the state of the law. Rather, in the absence of the feasibility of segregation under Article 58(a) and (b), governments accept the obligation of protection under Article 58(c).¹²³

IV. Alternative Responsibilities Under Article 58(c)

While cyber segregation is an overwhelming task, effective cyber protection is only slightly less daunting.¹²⁴ Understanding what Article 58(c)

120. 6 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE, *supra* note 91, at 214.

121. See Harris, *supra* note 6 (relating fears that Iraqi military communications networks were potentially connected to French banking networks); *supra* notes 9–12 and accompanying text.

122. See ARNAUD DE BORCHGRAVE ET AL., CTR. FOR STRATEGIC & INT’L STUDIES, CYBER THREATS AND INFORMATION SECURITY: MEETING THE 21ST CENTURY CHALLENGE 7 (2000) (estimating that in 2000, the rate of interconnectedness was 95%).

123. See API, *supra* note 8, art. 58(c) (requiring the government to take all other necessary precautions to protect civilians from the dangers of military operations).

124. See Sklerov, *supra* note 53, at 26. In analyzing the effectiveness of U.S. cyber protection, Lieutenant Commander Sklerov observes,

Unfortunately, computer security in its present form is not enough to stop cyberattacks. Computer software frequently has design flaws that open systems to attack, despite system administrators’ best efforts to fully secure their computer systems. These design flaws are compounded by administrator and user carelessness in both system design and use, which often nullify the security measures put in place to defend a system. Furthermore, poor design of federal computer networks has left them with more entry points than U.S. early warning programs can effectively monitor at one time, leaving U.S. computer systems vulnerable to attack until the amount of entry points is reduced. These vulnerabilities highlight the fact that passive defenses alone are not enough to protect states from cyberattacks.

Id. Sklerov advocates for the use of “active defenses” to protect critical computer networks and systems against states that do not prevent attacks from within their territory. *Id.*

does and does not require is vital to complying with the obligation it imposes. Based on the negotiating history already discussed and the plain reading of the text, it appears that there are three key concepts in the Article: “to the maximum extent feasible,” “other necessary precautions,” and “under their control.”¹²⁵ The first and last of these act to limit the extent of required government action, while the second acts to force otherwise deferred action.

In analyzing Article 58(c)’s application to cyber warfare, it is important to note the negotiators were clear that the language of “to the maximum extent feasible” applied to the entire Article, making the obligation to protect subject to this same caveat.¹²⁶ As one cyber expert recently stated, it is not possible to protect all the networks all the time.¹²⁷ Recognizing that it is not feasible to protect everything all the time requires some decision methodology. While some have argued for protection of critical national infrastructure as a top priority,¹²⁸ this category may be broader than the contours of Article 58 require. Each state will have to make its own determination as to what is feasible, but it is important to note that the language is the “maximum” extent, not the minimum.¹²⁹

The second concept that acts to limit the required government action is the language concerning control of civilians and civilian objects. The Article only requires governments to protect those civilians and civilian objects that are “under their control.”¹³⁰ Returning to the non-cyber example of the military use of the seaport, under Article 58(c), if certain civilians or civilian objects came under the control of the military at the seaport, the military would be obliged to take necessary precautions to protect those civilians and civilian objects from the dangers resulting from military operations, including attacks by the enemy.¹³¹ This might include actions such as segregating civilians and civilian objects as much as possible within the military portions of the seaport, placing civilian work spaces in protected areas such as in buildings or bunkers, or creating evacuation plans that would quickly move civilians to a safer location in the event of attack.

125. API, *supra* note 8, art. 58(c).

126. 14 OFFICIAL RECORDS OF THE DIPLOMATIC CONFERENCE, *supra* note 91, at 199.

127. Colonel Guillermo R. Carranza, Remarks at the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology (Feb. 6, 2010).

128. See Sean M. Condrón, *Getting it Right: Protecting American Critical Infrastructure in Cyberspace*, 20 HARV. J.L. & TECH. 404, 407 (2007) (asserting that critical infrastructure is vital to a nation’s survival and that a safe and secure cyber environment is necessary to support the critical infrastructure); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense*, 38 STAN. J. INT’L L. 207, 229 (2002) (arguing that the United States must “establish a domestic practice of protecting its critical national infrastructure” against computer-network attacks); Sklerov, *supra* note 53, at 26 (arguing that current computer security is not enough to stop cyber attacks and, as a consequence, states will feel the need to build active defenses).

129. API, *supra* note 8, art. 58.

130. *Id.*

131. *Id.*

Similarly, any computers, networks, systems, routers, telecom hotels, etc., would have to be under the control of the government to come under this obligation. Recall that during the negotiations this provision was meant to be understood as a *de facto* standard, not *de jure*.¹³² One scenario where this provision gives meaning to the obligation would be a cyber attack launched by an enemy where the government determined it was necessary to take control of a particular computer network, securing the portions necessary to ensure continuity of government operations. The network would continue to be a civilian object, though discrete military communications would be targetable.¹³³ Once the government took control of the network, it would have to accept the obligation to protect the entire network, including the civilian communications traffic.¹³⁴

Another example might be a telecom hotel through which valuable military communications pass between the continental United States and Europe. During an armed conflict, the government might take physical and cyber control to ensure its military communications were uninterrupted. Countless civilian communications would pass through that same telecom hotel, and the U.S. government would have to accept the obligation to protect those communications as well.

Finally, Article 58(c) requires the government to take “other necessary precautions.”¹³⁵ This language is significant for at least two reasons. First, the word “other” seems to indicate that the required actions may involve more than just additional segregation. In other words, if segregating under the preceding two paragraphs of Article 58 were not feasible, the government cannot meet the obligation of paragraph (c) merely by segregating those civilian cyber activities “under their control” and then leaving them to fend for themselves. Once the government accepts the obligation to protect, other “feasible” precautions are required.

Second, the use of the term “precautions” is significant. Precautions note actions taken in advance, not just in response.¹³⁶ This is particularly appropriate in the context of cyber warfare where an attack can happen in the time it takes to make a keystroke, sending a destructive stream of electrons into an enemy’s computer system. With a damaging cyber attack so instantaneous, the government cannot take this obligation as a reactionary responsibility. Rather, the government has to act in advance of a potential attack. And since no one knows when that potential attack will come, the

132. See *supra* notes 93–99 and accompanying text.

133. See *supra* notes 74–81 and accompanying text.

134. See API, *supra* note 8, art. 58 (requiring governments to protect civilian objects under their control from the dangers of military operations).

135. *Id.*

136. Precaution is “a measure taken beforehand to prevent harm or secure good.” MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY 976 (11th ed. 2003).

government has to act now to ensure potential civilian cyber activities that either are or will come under its control will be adequately protected.

This, then, becomes the crux of the requirement for the government. It requires some forethought and immediate action. It requires the government to analyze which of its cyber capabilities it will want to guarantee functionality when an armed conflict occurs. Then, the government must determine what civilian systems, companies, networks, etc., are necessary to maintain that functionality. Having made that determination, the government must act now to put the necessary steps in place to protect those civilians and civilian objects which will likely come under its control. Waiting until these systems are under attack will not meet the obligations of Article 58 and the law of armed conflict.¹³⁷ Immediate action is required.

One complicating factor is that such actions will require specific legal authority and significant cooperation with the private sector. As one commentator recently noted concerning cyber protection, “[T]he list of powers granted to the President in carrying out his duties as Commander in Chief is devoid of any authority to defend private industry.”¹³⁸ The next Part will review steps already taken by the government to ensure continuing cyber functionality in the face of an armed attack.

V. U.S. Practice in Protecting Civilians and Civilian Cyber Objects

Beginning in the 1990s, as the U.S. government’s use of the Internet increased and its dependence on the Internet for communication and functionality expanded, the need for protection became more apparent. The actions taken over the ensuing two decades have been detailed elsewhere¹³⁹ and need not be repeated here. However, it is worth drawing attention to several specific provisions or actions that delineate the government’s plans on protecting civilians and civilian objects from the effects of potential attacks.

Initially, the government’s predominant focus for protection was critical national infrastructure.¹⁴⁰ In hindsight, this decision seems prescient, as re-

137. See API, *supra* note 8, art. 58 (prescribing various mechanisms to be taken by the parties to a conflict to protect individuals from the effects of attacks).

138. Todd A. Brown, *Legal Propriety of Protecting Defense Industrial Base Information Infrastructure*, 64 A.F. L. REV. 211, 220 (2009).

139. See *id.* at 219–20 (discussing the Homeland Security Act of 2002); Kastenberg, *supra* note 67, at 48–50 (describing various executive and legislative initiatives taken to safeguard U.S. infrastructure); Sklerov, *supra* note 53, at 25–26 (outlining efforts to ensure that the private sector acts on both computer security and a government early-warning system for cyber attacks); U.S. DEP’T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN 185 app. 2 (2009), http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf [hereinafter NIPP] (containing a comprehensive list of U.S. statutes, strategies, and directives dealing with infrastructure protection).

140. “Critical infrastructure” is defined in the relevant U.S. Code as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such

cent history has shown an ever-increasing focus of attacks on critical infrastructure.¹⁴¹ In 1997, President Clinton created the President's Commission on Critical Infrastructure Protection and followed in 1998 by issuing Presidential Decision Directive 63, concerning protection of U.S. critical infrastructure.¹⁴² The Directive made it the policy of the U.S. government to "take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."¹⁴³ The Directive recognized the need for strong public-private partnership and urged that "[s]ince the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector."¹⁴⁴

In 2002, Congress passed the Homeland Security Act, which authorized the President and the Secretary of Homeland Security to designate critical-infrastructure-protection programs.¹⁴⁵ As a result of this authority, the President "issued a number of directives designating critical infrastructure protection programs and describing responsibilities therein."¹⁴⁶ One of these directives was the Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection¹⁴⁷ (HSPD-7). Issued in December of 2003, HSPD-7 states very clearly the policy of the United States at least with regard to protection of critical infrastructure from terrorist attacks:

It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could:

- (a) cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;
- (b) impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;
- (c) undermine State and local government capacities to maintain order and to deliver minimum essential public services;

systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e) (2006).

141. See Press Release, *supra* note 37 (noting cyber attacks on the White House, DHS, U.S. Secret Service, and DOD).

142. Memorandum on Critical Infrastructure Protection, Presidential Decision Directive/NSC-63 (May 22, 1998), available at <http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf>.

143. *Id.* at 2.

144. *Id.* at 3.

145. Homeland Security Act of 2002, Pub. L. No. 107-296, § 213, 116 Stat. 2135, 2152 (codified at 6 U.S.C. § 132 (2006)).

146. Brown, *supra* note 138, at 220.

147. 39 WEEKLY COMP. PRES. DOC. 1816 (Dec. 17, 2003).

- (d) damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
- (e) have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or
- (f) undermine the public's morale and confidence in our national economic and political institutions.¹⁴⁸

As directed in HSPD-7, the government created a National Infrastructure Protection Plan (NIPP) in 2006 and updated it in 2009.¹⁴⁹ Within the NIPP, the DOD was assigned as the Sector Specific Agency (SSA) for the Defense Industrial Base (DIB).¹⁵⁰ As the SSA for the DIB, DOD has the responsibility to "implement the NIPP sector partnership model and risk management framework; develop protective programs, resiliency strategies, and related requirements; and provide sector-level [critical infrastructure and key resources (CIKR)] protection guidance in line with the overarching guidance established by DHS pursuant to HSPD-7."¹⁵¹ Also, the NIPP discusses the National Infrastructure Inventory, a "national inventory of the assets, systems, and networks that make up the nation's CIKR."¹⁵²

As part of its responsibility under the NIPP, DOD issued its sector-specific plan for the DIB (DIB SSP) in May 2007.¹⁵³ One of the key points in the plan is that "[p]rivate sector participation in executing the NIPP is voluntary."¹⁵⁴ The DIB SSP acknowledges that "[c]urrently, there are no regulatory requirements for conducting formal risk assessments" within the DIB.¹⁵⁵ In fact, critical-infrastructure executives in the United States reported the "lowest levels" of government regulation across the fourteen countries surveyed.¹⁵⁶ In response, DOD has conducted risk assessments on portions of the DIB of its own accord.¹⁵⁷ However, DOD admits that it is not conducting comprehensive risk assessments on the DIB in the area of cyber assets. The DIB SSP states, "While cyber security is an issue that could affect any facility, DOD does not perform network- or system-level assessments."¹⁵⁸

148. *Id.* at 1817.

149. NIPP, *supra* note 139, at 7–8.

150. *Id.* at 19.

151. *Id.* at 18.

152. *Id.* at 29.

153. U.S. DEP'T OF DEF., DEFENSE INDUSTRIAL BASE: CRITICAL INFRASTRUCTURE AND KEY RESOURCES SECTOR-SPECIFIC PLAN AS INPUT TO THE NATIONAL INFRASTRUCTURE PROTECTION PLAN (2007), available at <http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf>.

154. *Id.* at 4.

155. *Id.* at 17.

156. BAKER ET AL., *supra* note 24, at 1.

157. U.S. DEP'T OF DEF., *supra* note 153, at 17.

158. *Id.*

In February 2003, the President issued the National Strategy to Secure Cyberspace.¹⁵⁹ While this strategy encourages public-private coordination on securing critical infrastructure, it also expands the scope of government concern to include “reduc[ing] our national vulnerabilities to cyber attack.”¹⁶⁰ Enlarging the aperture by which the government is directing policy from critical infrastructure to national vulnerabilities is laudable. However, the strategy also states that “[t]he federal government could not—and, indeed, should not—secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector.”¹⁶¹

In 2008, President Bush also issued NSPD-54/HSPD-23 creating the Comprehensive National Cybersecurity Initiative.¹⁶² This NSPD takes a broader view than just critical infrastructure, though it is mostly focused on government networks.¹⁶³ Though the NSPD is not available to the public, one commentator recently stated,

President Bush, by means of a classified directive signed on 8 January 2008, authorized federal intelligence agencies, in particular the National Security Agency (NSA), to monitor the computer networks of all federal agencies, including those they had not previously monitored. Pursuant to this directive, a task force headed by the Office of the Director of National Intelligence (ODNI) will coordinate efforts to identify the source of cyber-attacks against government computer systems. The DHS and DOD will take ancillary roles in this effort—protecting systems and devising strategies for counterattacks.¹⁶⁴

In March of 2009, the GAO released a report on National Cybersecurity Strategy.¹⁶⁵ The report finds that “DHS has yet to fully satisfy its cybersecurity responsibilities designated by the [2003 National Strategy to Secure Cyberspace].”¹⁶⁶ The report does admit some progress in many areas,

159. WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf. In 2004, President Bush issued National Security Presidential Directive 38 (NSPD-38), also called the National Strategy to Secure Cyberspace. The 2004 document is not available to the general public due to its classification.

160. *Id.* at 14.

161. *Id.* at 11.

162. JOHN ROLLINS & ANNA C. HENNING, CONG. RESEARCH SERV., COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS 1 (2009).

163. *See id.* at 7 (“[T]he primary response and recovery activities associated with previous [private] network breaches have been addressed by the private sector entity that has been the victim of the attack.”).

164. Brown, *supra* note 138, at 240–41; *see also* Ellen Nakashima, *Bush Order Expands Network Monitoring*, WASH. POST, Jan. 26, 2008, at A3 (providing additional description of the directive issued by President Bush).

165. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-432T, NATIONAL CYBERSECURITY STRATEGY: KEY IMPROVEMENTS ARE NEEDED TO STRENGTHEN THE NATION'S POSTURE (2009).

166. *Id.* at 4.

but also contains twelve recommendations that still need attention.¹⁶⁷ One of those recommendations is to “[f]ocus more actions on prioritizing assets and functions, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.”¹⁶⁸ The report goes on to say,

[E]fforts to identify which cyber assets and functions are most critical to the nation have been insufficient [I]nclusion in cyber critical infrastructure protection efforts and lists of critical assets are currently based on the willingness of the person or entity responsible for the asset or function to participate and not on substantiated technical evidence.¹⁶⁹

Shortly after entering office, President Obama ordered a comprehensive review of the U.S. cyber strategy.¹⁷⁰ This review resulted in the Cyberspace Policy Review.¹⁷¹ The Review argued,

The Federal government cannot entirely delegate or abrogate its role in securing the Nation from a cyber incident or accident. The Federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and well-being of citizens. The private sector, however, designs, builds, owns, and operates most of the digital infrastructures that support government and private users alike. The United States needs a comprehensive framework to ensure a coordinated response by the Federal, State, local, and tribal governments, the private sector, and international allies to significant incidents.¹⁷²

In light of Article 58 obligations, this framework should include the protection of certain civilian networks and systems from the effects of attacks.

Among the many recommendations made in the Review, perhaps the most pertinent to this Article concerns the protection of private networks:

The Federal government should work with the private sector to define public-private partnership roles and responsibilities for the defense of privately owned critical infrastructure and key resources. The common defense of privately-owned critical infrastructures from armed attack or from physical intrusion or sabotage by foreign military forces or international terrorists is a core responsibility of the Federal government. Similarly, government plays an important role in protecting these infrastructures from criminals or domestic terrorists. The question remains unresolved as to what extent protection of these

167. *Id.* at 6–12.

168. *Id.* at 9.

169. *Id.* at 10.

170. *Id.* at 4.

171. WHITE HOUSE, CYBERSPACE POLICY REVIEW (2009), available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

172. *Id.* at iv–v.

same infrastructures from the same harms by the same actors should be a government responsibility if the attacks were carried out remotely via computer networks rather than by direct physical action. Most private network operators and service providers consider it to be their responsibility to maintain and defend their own networks, but key elements of the private sector have indicated a willingness to work toward a framework under which the government would pursue malicious actors and assist with information and technical support to enable private-sector operators to defend their own networks.¹⁷³

The DOD has also been actively pursuing its abilities to defend cyberspace, including civilian elements that are necessary to support military capabilities. In a recent address, Deputy Secretary of Defense William Lynn stated, “[T]he Defense Department has formally recognized cyberspace for what it is—a domain similar to land, sea, air and space. A domain that we depend upon and must protect.”¹⁷⁴ He continued,

Our defenses need to be dynamic. A fortress mentality will not work in cyber. We cannot retreat behind a Maginot line of firewalls. Cyber war is much more like maneuver warfare, and these new technologies help us find and neutralize intrusions. But we must also keep maneuvering. If we stand still for a minute our adversaries will overtake us.¹⁷⁵

It may be that the majority of cyber attacks against U.S. systems come from private individuals, but as CSIS reported in its report for the incoming President, “Our most dangerous opponents are the militaries and intelligence services of other nations.”¹⁷⁶ To help respond to the increasing capability and lethality of cyber attacks, Defense Secretary Robert Gates announced in June 2009 the creation of U.S. Cyber Command, which will be tasked with “protecting and coordinating the nation’s computer and defense networks and infrastructure.”¹⁷⁷ According to Deputy Secretary Lynn,

Cyber Command will bring together more than half a dozen intelligence and military organizations in support of three overlapping categories of cyber operations. First, CYBERCOM will lead the day to day defense and protection of all DoD networks, raising our situational awareness and control. Second, CYBERCOM will coordinate all DoD network operations providing full spectrum

173. *Id.* at 28.

174. Lynn, *supra* note 41.

175. *Id.*

176. COMM’N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, *supra* note 38, at 13; see also Elinor Mills, *Report: Countries Prepping for Cyberwar*, CNN, Nov. 16, 2009, <http://www.cnn.com/2009/TECH/11/17/cnet.cyberwar.internet/index.html?iref=allsearch> (suggesting that countries and nation-states are gearing up their offensive “cyberweapon” capabilities and may already be engaged in attacks on networks).

177. Ryan Justin Fox, *Fort Meade to Be Cyber Defense Home*, CAPITAL, Oct. 12, 2009, available at <http://www.hometownannapolis.com/news/top/2009/10/12-14/Fort-Meade-to-be-cyber-defense-home.html>.

support to military and counter-terrorism missions. Third, CYBERCOM will stand by to support civil authorities and industry partners on an as-needed basis.¹⁷⁸

The new Cyber Command falls under Strategic Command or STRATCOM, one of the unified and specified commands created by statute to conduct the nation's warfighting.¹⁷⁹ "Part of USSTRATCOM's mission is to ensure freedom of action in cyberspace and to deliver integrated kinetic and non-kinetic effects, including information operations, in support of Joint Force Commander operations."¹⁸⁰ This freedom of action would certainly include the ability to use certain civilian networks in times of armed conflict.

It is clear that the government is taking important steps to include critical civilian networks, systems, and infrastructure under its protective umbrella.¹⁸¹ However, there are three consistent problems with the government's approach. The first is that a majority of these plans and policies depend on the voluntary assent of the private sector. This includes relying on the civilian sector to assess vulnerabilities and execute solutions. Second, the consistent approach throughout these policies and plans is reactive, not proactive. Remediation and damage management are consistent themes, with only little attention to prevention, detection, and protection. Finally, these plans and policies do not assign the appropriate role for DOD, given the potential for cyber attack as part of armed conflict.

In the absence of a legal obligation, allowing the private sector to govern itself may be appropriate to some degree. However, given the government's legal obligation imposed by Article 58 to protect civilian objects under government control during times of armed conflict, a voluntary regime is not sufficient. In failing to make assessments mandatory, these plans and policies leave the government in the situation of not knowing the complete scope of the problem—who they need to protect and to what extent.¹⁸² HSPD-7's authorization for DHS to provide protection and guidance to the private sector¹⁸³ carries no mandatory compliance requirements and is insufficient to meet the United States' legal obligations. The 2003 National Strategy to Secure Cyberspace's statement that the government "should not" secure private-sector systems denotes a lack of acceptance

178. Lynn, *supra* note 41.

179. See 10 U.S.C. § 161 (2006) (authorizing the creation of commands to conduct military missions).

180. Schaap, *supra* note 1, at 130.

181. See *supra* notes 171–73 and accompanying text.

182. See *supra* note 169 and accompanying text.

183. See Homeland Security Presidential Directive 7, *supra* note 147, at 1817 ("Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective.").

of the responsibility under Article 58.¹⁸⁴ As long as participation in the government's cybersecurity plan is voluntary, the results will be uneven and insufficient. The Cyberspace Policy Review had it exactly right when it said that "[t]he common defense of privately-owned critical infrastructures from armed attack or from physical intrusion or sabotage by foreign military forces or international terrorists is a core responsibility of the Federal government."¹⁸⁵ The government needs to listen and respond.

Additionally, throughout the DIB SSP, it is clear that the government takes a reactive approach to asset protection. In laying out a strategy for layered defense, the federal government is the fifth (and last) level and is appropriate only after local authorities, state or local law enforcement, and the state's national guard or other federal agencies have all failed, and the President determines it is then appropriate to use military assets.¹⁸⁶ Though the DIB SSP states that it is DOD's goal to prevent and detect potential incidents,¹⁸⁷ there is no requirement for members of the DIB to support this goal or take any actions at all toward this end. This approach is insufficient in a technological age where the attack can be an instantaneous burst of electrons that will destroy or significantly degrade the cyber capabilities of a critical infrastructure that the United States may be obliged to protect. NSPD-54's requirement of monitoring is a step in the right direction, but it falls short of providing the protection required under Article 58.¹⁸⁸

Finally, while perhaps the focus on terrorist attacks can be overlooked since HSPD-7 was promulgated in the wake of the September 11 attacks,¹⁸⁹ the current government approach fails to recognize the central role DOD will have to play in response to a cyber attack. This sentiment is echoed in a 2007 GAO report, where the GAO found that "DOD relies so heavily on non-DOD infrastructure assets that their unavailability could critically hinder the DOD's ability to project, support, and sustain forces and operations worldwide."¹⁹⁰ The report's assumption that protection from armed attack, even of private critical networks, was the responsibility of the government is

184. See WHITE HOUSE, *supra* note 159, at 11. In reference to the government's responsibility in cybersecurity, the policy states,

The federal government could not—and, indeed, should not—secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector. . . . Each American who depends on cyberspace, the network of information networks, must secure the part that they own or for which they are responsible.

Id.

185. WHITE HOUSE, *supra* note 171, at 28.

186. U.S. DEP'T OF DEF., *supra* note 153, at 23.

187. *Id.* at 24.

188. See *supra* text accompanying note 164.

189. See *supra* text accompanying notes 145–48.

190. Brown, *supra* note 138, at 234 (citing U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-461, DEFENSE INFRASTRUCTURE: ACTIONS NEEDED TO GUIDE DOD'S EFFORTS TO IDENTIFY, PRIORITIZE, AND ASSESS ITS CRITICAL INFRASTRUCTURE 1 (2007)).

a recognition of the same principles Article 58 enshrines, and DOD will be the primary government actor to provide that protection.¹⁹¹ When armed conflict begins and cyber attacks hit U.S. networks, the President is not going to turn to DHS and ask what it is doing about it. The responsibility is going to fall to DOD. The government needs to embrace that reality now and adjust its plans and policies accordingly.

VI. Recommendations

In his speech quoted at the beginning of this Article, which was given in response to the Cyberspace Policy Review, President Obama acknowledged the need for greater work to protect the United States' communications capabilities.¹⁹² The nature of the Internet prevents effective post-attack protection when facing the instantaneous degradation of cyber capabilities. To effectively protect civilian networks and systems in accordance with the United States' obligations under Article 58(c), the government must take affirmative steps now. The following six recommendations will do much to bring the United States in compliance with its Article 58 obligations.

First, the President, through DOD, should identify those civilian systems, networks, and industries that will become legitimate military targets in time of armed conflict because of their nature, location, purpose, or use. The President also needs to identify those that may come under the control of the government but not become military objectives.

President Obama's Cyberspace Policy Review has already recognized that "with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights. The government has a responsibility to address these strategic vulnerabilities."¹⁹³ Under the DIB SSP, DOD is already compiling information on critical infrastructure.¹⁹⁴ Additional analysis comparing military operations and plans against this information should yield a fairly accu-

191. See, e.g., U.S. DEP'T OF DEF., *supra* note 153, at 2 (noting that DOD is "the SSA responsible for collaboration with the DIB security partners, conducting or facilitating DIB vulnerability assessments, and encouraging risk management strategies to protect and mitigate the effects of attacks").

192. Obama, *supra* note 1. President Obama stated,

First, working in partnership with the communities represented here today, we will develop a new comprehensive strategy to secure America's information and communications networks. To ensure a coordinated approach across government, my Cybersecurity Coordinator will work closely with my Chief Technology Officer, Aneesh Chopra, and my Chief Information Officer, Vivek Kundra. To ensure accountability in federal agencies, cybersecurity will be designated as one of my key management priorities. Clear milestones and performance[] metrics will measure progress.

Id.

193. WHITE HOUSE, *supra* note 171, at i.

194. U.S. DEP'T OF DEF., *supra* note 153, at 23, 25.

rate assessment. This assessment will provide the baseline for specific actions required to comply with Article 58.

Second, Congress and the President should expand the current policy and authorities, such as HSPD-7, to include protection not just from terrorists, but from state parties in armed conflicts. Congress should provide the Executive specific authority to protect those privately owned industries, systems, and networks that are anticipated to come under the control of the government during times of armed conflict. Part of this authority should include methods to monitor, implement, and enforce cybersecurity and survivability measures in those specific networks, systems, and industries now.

Such action is not without precedent. Congress has authorized the President to take similar actions with communications systems in times of armed conflict in the past.¹⁹⁵ Current law is insufficient to do so in the current age against the current threats.¹⁹⁶ Former Clinton Deputy Attorney General Jamie S. Gorelick recently urged the Obama Administration to “seek legislation for comprehensive authority to deal with a cyber emergency” including monitoring or cutting off private cell phones and other communications devices.¹⁹⁷ President Obama has shown a reluctance to take steps that invade personal privacy.¹⁹⁸ These situations are not mutually exclusive. Monitoring those systems selected above and taking necessary steps to

195. WHITE HOUSE, *supra* note 171, at C-4 to C-5. According to the Review,

Recognizing the pivotal importance of communications to support the execution of government functions during a crisis, Congress, by joint resolution in 1918, authorized the President to assume control of any telegraph, telephone, marine cable or radio system or systems in the U.S. and to operate them as needed for the duration of World War I. Relying on this Congressional authorization, President Wilson issued a proclamation asserting possession, control and supervision over every telegraph and telephone system within the United States. To preserve support for critical government communications needs during times of crisis, Congress later included in Section 706 of the Communications Act of 1934 authority for the President to control private communications systems within the United States during wartime.

Id.

196. *See id.* at 17 (“Current law permits the use of some tools to protect government but not private networks, and vice versa.”).

197. *See* Ellen Nakashima, *War Game Reveals U.S. Lacks Cyber-Crisis Skills*, WASH. POST, Feb. 17, 2010, at A3 (warning that Americans should not expect their “cellphone and other communications to be private—not if the government is going to have to take aggressive action to tamp down the threat”).

198. *See* Obama, *supra* note 1 (stressing the importance of maintaining personal privacy and net neutrality). President Obama remarked,

Let me also be clear about what we will not do. Our pursuit of cybersecurity will not—I repeat, will not include—monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans. Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be—open and free.

Id. *But see* Geoff Fein, *Effort Underway to Put Network Security Language into DFAR*, DEF. DAILY, July 8, 2009, available at 2009 WLNR 14424861 (stating that there is an effort to “define in both the [Defense Federal Acquisition Regulations] and the Federal Acquisition Regulations (FAR) what kind of network infrastructure is needed”).

ensure their protection does not have to include invasions of privacy. Congress can provide authority and the President can implement that authority in a way that will meet our legal obligations; protect the necessary networks, systems, and industries; and preserve our individual rights.

Third, the President, after identifying those industries, networks, and systems that will become targetable and using the additional authority granted by Congress, should establish memoranda of agreement with these private entities to ensure sufficient protection of these industries and networks. This does not mandate government intrusion in civilian networks, industries, or systems. The government can establish the standard, put in place necessary safeguards, and establish effective monitoring systems and then allow these civilian entities to provide their own protection or opt for some combination of government and private security. Whatever method is agreed upon, the government should determine the sufficiency of the protection and then monitor implementation of the protective measures and have the authority to enforce compliance if necessary.

Prior work in the public-private partnership area already has set an effective base for this action. IT and security executives in the United States reflected the highest confidence level (73%) in the ability of their government to deter cyber attacks of any of the surveyed countries.¹⁹⁹ But the current “voluntary” nature of this partnership does not go far enough. Former Assistant Secretary of DHS Stewart Baker believes that “the private sector [is] not prepared to defend against a cyber act of war and that the government need[s] to play a role.”²⁰⁰ Government involvement and regulation has proven to be one of the most effective means to incentivize the private sector to improve security.²⁰¹ In those specific areas where the government anticipates the obligation to protect civilian objects during armed conflict, the government has to be able to take a more proactive role to ensure the proper protections are in place before the attack occurs and the systems are degraded.

Again, President Obama has shown some reluctance to move in this direction. He recognizes the need for public-private partnership but hesitates to dictate specific standards for private companies.²⁰² This hesitation may be

199. See BAKER ET AL., *supra* note 24, at 26 (reporting that only 27% of U.S. IT and security executives think the U.S. government is “not capable or not very capable” of deterring cyber attacks).

200. Nakashima, *supra* note 197.

201. See BAKER ET AL., *supra* note 24, at 39 (“For owners and operators, . . . their relationships to governments are a key factor in how they handle security. For governments, that relationship is crucial for the defense of national assets. In the absence of technological silver bullets, many executives see regulation—despite its drawbacks—as a way of improving security.”).

202. See Obama, *supra* note 1. Indeed, the President has stated,

Third, we will strengthen the public/private partnerships that are critical to this endeavor. The vast majority of our critical information infrastructure in the United States is owned and operated by the private sector. So let me be very clear: My

well-placed generally, but in the face of a legal obligation to protect those limited civilian objects under the control of the government in times of armed conflict, and potential catastrophic consequences for failure, the current paradigm falls short.

Fourth, the government should establish and maintain a “hack back” or other technological solution that protects those systems and networks designated by the President that will come under government control during armed conflict. Many scholars agree that “[a]ctive defenses are the most appropriate type of force to use against cyberattacks in light of the principles of *jus in bello*.”²⁰³ A hack-back-type technology will serve as a “credible military presence in cyberspace to provide a deterrent against potential hackers”²⁰⁴ in an area where deterrents are few. There is evidence that many corporations are already using hack back as a defensive option, including many Fortune 500 corporations.²⁰⁵

Such technological solutions may be limited at present and will need to continue to evolve as attacks evolve. Nearly every panel or review commissioned in the area of cybersecurity has argued that the government needs to invest more heavily in defensive cyber-war capabilities.²⁰⁶ President Obama seems to have embraced the need for increased spending,²⁰⁷ but must also

administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity.

Id.

203. Sklerov, *supra* note 53, at 79; *see also* Jensen, *supra* note 83, at 232–39 (taking the position that in order to combat cyber attacks “the law should permit an active response based on the target of the attack”).

204. COMM’N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, *supra* note 38, at 23.

205. Ruperto P. Majuca & Jay P. Kesan, *Hacking Back: Optimal Use of Self-Defense in Cyberspace* 5–6 (Ill. Pub. Law & Legal Theory Papers Series, Research Paper No. 08-20, 2009), available at <http://papers.ssrn.com/abstract=1363932> (“[A] survey of 320 Fortune 500 corporations revealed that around 30% of the companies have installed software capable of launching counterattack measures.”). *But see* ROSENZWEIG, *supra* note 21, at 18 (speculating that a hack back response would probably violate domestic law).

206. *See, e.g.*, U.S. GOV’T ACCOUNTABILITY OFFICE, *supra* note 165, at 11 (“[E]xperts stated that the U.S. is not adequately focusing and funding research and development efforts to address cybersecurity or to develop the next generation of cyberspace to include effective security capabilities.”); WHITE HOUSE, *supra* note 159, at 34 (“Federal investment in research for the next generation of technologies to maintain and secure cyberspace must keep pace with an increasing number of vulnerabilities.”); COMM’N ON CYBERSECURITY FOR THE 44TH PRESIDENCY, *supra* note 38, at 74 (lamenting as inadequate the government’s 2009 allocation of \$300 million toward research and development in cybersecurity); MARTIN C. LIBICKI, RAND CORP., CYBERDETERRENCE AND CYBERWAR 159 (2009), http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf (arguing that the DOD will need to spend far more on cybersecurity defense than offense).

207. *See* Obama, *supra* note 1. With respect to investing in cybersecurity, the President has stated,

Fourth, we will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet the digital challenges of our time. And that’s why my administration is making major investments in our information infrastructure: laying broadband lines to every corner of America; building a smart electric grid to deliver energy more efficiently; pursuing a next generation of

make a commitment to the hack back technology as a deterrent and first line of protection for specifically designated networks and systems.²⁰⁸

Fifth, the government should create a strategic reserve of Internet capability, including bandwidth, routers, and other necessary means. This would be much like the strategic petroleum reserve whose purpose is to “provide[] the President with a powerful response option should a disruption in commercial oil supplies threaten the U.S. economy.”²⁰⁹ A “strategic cyber reserve” would ensure that critical cyber networks and systems have a place to go when they are being attacked.

In the armed conflict between Russia and Georgia, after the Georgian government sites were shut down by attackers, the Georgian government was able to reestablish itself on servers hosted outside its own borders.²¹⁰ Obviously, the scale of the cyber reserve would need to be sufficient to preserve vital U.S. interests and protect those civilian systems and networks that fall under Article 58.

Finally, the government should push the international community for greater recognition of each state’s requirement under international law to not allow its territory to be used for acts harmful to another state.²¹¹ This “no harm” principle places the responsibility to stop attacks on the country from which they originate or through which they are passed. In several recent attacks, countries from which the attacks have originated refused to accept responsibility and even refused to cooperate with investigations.²¹² That is unacceptable.²¹³

The Cyberspace Policy Review argued that “[i]nternational norms are critical to establishing a secure and thriving digital infrastructure. The United States needs to develop a strategy designed to shape the international

air traffic control systems; and moving to electronic health records, with privacy protections, to reduce costs and save lives.

Id.

208. Mike McConnell, *To Win the Cyber War, Look to the Cold War*, WASH. POST, Feb. 28, 2010, at B1; see also Neville-Jones, *supra* note 47 (arguing, in a statement for the United Kingdom Conservative Party, that passive defenses are not sufficient to adequately protect against cyber attack).

209. U.S. Department of Energy, U.S. Petroleum Reserves, <http://www.fossil.energy.gov/programs/reserves/> (last updated Apr. 11, 2010).

210. Gorman, *supra* note 51.

211. See Sklerov, *supra* note 53, at 12–13 (arguing that requiring a host state to “hunt down [cyber] attackers within its borders” would allow victim states to “impute state responsibility to host-states that neglected this duty, and respond in self-defense”). *But see* ROSENZWEIG, *supra* note 21, at 14–15 (suggesting that there are many potential problems with blaming states for the actions of cyber attackers, including determining whether the state had sufficient control over the cyber attackers and dealing with cyber attacks that originate from multiple states).

212. Sklerov, *supra* note 53, at 6–10.

213. See Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1053–57 (2007) (advocating the need for international law to govern activities such as cyber attacks).

environment and bring like-minded nations together on a host of issues, including acceptable norms regarding territorial jurisdiction, sovereign responsibility, and use of force.”²¹⁴ The acceptance of the no harm principle is one such norm that should be embraced and specifically applied to cyber operations.

The value of this final suggestion in relation to Article 58 may seem tenuous because Article 58 obligations are only triggered in armed conflict. However, it is clear from recent events that armed conflicts need not come only from nation-states. In fact, terrorist organizations and other non-state actors can create an armed conflict.²¹⁵ Attacks from non-state actors are going to be conducted through the territory of a nation-state. A recognized requirement or international agreement for neutral states to interrupt harmful cyber activities from within their borders will indirectly provide protections for those civilian objects covered by Article 58.

Embracing these six recommendations will cause the government to adapt its current approach to cybersecurity. It will generate some resistance from the private sector. But it will also bring the United States into compliance with its law-of-armed-conflict obligation to protect civilians and civilian objects from the effects of cyber attacks.

VII. Conclusion

In the face of an armed conflict, including a cyber attack, the government cannot allow the collapse of civilian communications infrastructure to prevent an adequately coordinated and effective response to that armed attack. The government will have to step in to ensure continued connectivity. In doing so, it will inevitably rely on civilian industry and use civilian networks and systems to carry its important communications and to accomplish many vital national-security tasks, making these same industries, networks, and systems targetable by the enemy. It will also endanger civilian systems, networks, and industries that are not legitimate military objectives but may be collateral damage from an enemy’s attack of military objectives. Article 58(c) requires the government to protect those civilian networks and systems that come under its control to the maximum extent possible.²¹⁶

214. WHITE HOUSE, *supra* note 171, at 20. *But see* ROSENZWEIG, *supra* note 21, at 6 (“[T]he single greatest difficulty encountered thus far in the development of a legal response [to threats in cyberspace] lies in the transnational nature of cyberspace and the need to secure international agreement for broadly applicable laws controlling offenses in cyberspace.”).

215. In response to the attacks on the United States on September 11, 2001, the United Nations Security Council passed Resolution 1368, which recognizes the inherent right of self-defense that was triggered by the terrorist attacks. S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 12, 2001); *see also* S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001); NATO, NATO and the Fight Against Terrorism, http://www.nato.int/cps/en/natolive/topics_48801.htm (last updated May 4, 2010) (discussing NATO’s invocation of the collective-defense provision of the Washington Treaty, which can only be done in response to an armed attack).

216. *See supra* Part IV.

Article 58 of the API places an affirmative obligation on those facing attack to either segregate or protect civilians and civilian objects to the maximum extent feasible in order to spare them from the effects of attacks.²¹⁷ The application of Article 58 to cyber warfare was clearly not contemplated by the drafters who thought of this provision in territorial or geographic terms. However, in modern society, cyberspace has become not only an integral and necessary part of daily life but also a popular vehicle of both personal and military attack.

In applying Article 58 to cyber warfare, the near-complete interconnectedness of government and civilian cyber systems makes segregation under Article 58(a) and (b) impractical. Therefore, states must embrace the requirement under Article 58(c) to protect civilians and civilian objects under their control from the effects of attacks.

The United States has already taken steps to integrate the public- and private-sector defense strategies, particularly in the area of critical infrastructure. However, much more can and needs to be done. By following the six recommendations contained in Part VI, the government will not only bring itself into compliance with Article 58's obligations, but it will also be creating a safer and more resilient cyber world in the face of terrorist and other threats.

217. *See supra* notes 85–108 and accompanying text.

Sovereign Discourse on Cyber Conflict Under International Law

Sean Kanuck*

I. Introduction

This Article will expand the Symposium's dialogue on law, information technology, and national security in two ways: first, by examining the intersection of those three subjects through the optic of public international law versus domestic statutes, regulations, or case law; and second, by providing broader context for the related legal and policy challenges that are simultaneously confronting many countries. A global perspective on these issues is essential because no single nation's declaratory policy or legal interpretations will be binding on the international community. Moreover, law will be but one factor in determining how nation-states ultimately manage cyber conflicts among themselves in the future.

Efforts to analyze "information warfare" under international law began in the 1990s,¹ and since then, numerous governmental, military, academic, and corporate commentators around the world have expressed their personal or organizational views.² However, the international community itself has yet to reach collective conclusions regarding many aspects of law in cyberspace, including what constitutes an act of aggression or use of force in cyberspace.³ Those legal ambiguities are only exacerbated by the

* Harvard University, A.B., J.D.; London School of Economics, M.Sc.; University of Oslo, LL.M.; co-author of the 2009 White House Cyberspace Policy Review; member of the United States delegation to the 2009–2010 United Nations group of governmental experts on information security. The views expressed herein do not necessarily reflect the official position of the U.S. Government, the United Nations, or any of their respective subdivisions; accordingly, all statements of fact and opinion should be attributed solely to the author. The author wishes to thank Professor Robert Chesney for the invitation to participate in this Symposium and the Texas Law Review staff for its assistance in researching and editing this Article.

1. See, e.g., Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 889 n.7 (1999) (citing several earlier publications that also explored international law and cyber warfare).

2. See, e.g., NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 241–82 (William A. Owens et al. eds., 2009) [hereinafter NATIONAL RESEARCH COUNCIL] (analyzing cyber warfare under various principles and sources of international law).

3. U.S. President Barack Obama recognized this fact in a White House report which stated, "The Nation also needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force." WHITE HOUSE, CYBERSPACE POLICY REVIEW, at iv (2009), available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. Furthermore, the United Nations group of governmental experts that met during 2004–2005 failed to reach any

technological limitations that currently preclude definitive attribution of cyber events within the timeframe that would be required for national-command-authority decisions in the face of genuine military attacks.⁴ With those dual uncertainties—legal and practical—in mind, states are striving to protect their national security interests and critical information infrastructures.

The threefold objectives of this Article are to (1) elucidate how cyberspace and cyber conflicts are currently being considered by sovereign governments, (2) identify related and unresolved areas of public international law, and (3) describe the strategic dynamic of state practice as it pertains to cyberspace. This Article will not, on the other hand, review the secondary literature in detail, evaluate the legal arguments of any specific nation, or offer a comprehensive framework from the internationalist perspective. The purpose herein is to raise awareness of—rather than critique—the sovereign decisions that are being made within national governments and multilateral organizations as well as their potential impact. Accordingly, the normative discussion will be limited to a single, preambulatory admonition that government and military officials in every nation should have the requisite knowledge to be fully cognizant of the international legal ramifications of the actions they take.⁵ Without such circumspection, they may inadvertently set precedents that could lead to increased insecurity for their own countries and the global community at large.⁶

consensus on possible cooperative measures to address potential threats in the sphere of information security. See The Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 5, delivered to the General Assembly, U.N. Doc. A/60/202 (Aug. 5, 2005) (“[G]iven the complexity of the issues involved, no consensus was reached on the preparation of a final report.”).

4. See WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE, at viii (2003), available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (“The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all.”); A.A. Streltsov, *International Information Security: Description and Legal Aspects*, DISARMAMENT F., 2007 (Issue 3), at 11 (stating Russia’s similar assessment that “it would be challenging to determine whether the attacker was acting in an individual capacity, or on behalf of a criminal organization, the government or armed forces”).

5. In the United States, for example, few of the government and military attorneys formulating policy in this area have studied international law overseas or practiced in a foreign legal system. They are predominantly specialists in U.S. administrative law who—owing to both their exclusive training in the Anglo-American common law tradition and their professional focus on domestic legislation and regulatory policy—are unaccustomed to the particular sources, procedures, and modes of legal reasoning employed in public international law. That inexperience also limits their ability to assess how foreign governments will interpret and apply those same provisions.

6. See *infra* note 63 and accompanying text.

II. Territorial Sovereignty

A. *Misnomer of a Virtual Jurisdiction*

Although some futurists might argue that cyberspace constitutes a realm unto itself which exists beyond all territorial boundaries and cannot be regulated, nation-states do strive to exercise their sovereignty over cyberspace—albeit ineffectively at times.⁷ The physical location of actors, victims, and the technical nodes that connect them are of central importance because governments continue to address cyber conflicts involving both state and nonstate actors as matters to be resolved by sovereign powers under their respective legal systems or through bilateral or multilateral agreements with other governments.⁸ In the case of cybercrime, for instance, those events that cannot be adequately investigated by local law enforcement authorities or fully prosecuted under domestic criminal systems find recourse to transnational judicial cooperation via mutual-legal-assistance treaties and multilateral organizations, such as the International Criminal Police Organization (INTERPOL).⁹ Furthermore, the nature of the international legal system affords this sovereign-centric approach primacy under the United Nations (U.N.) Charter regime.¹⁰

Every component of every information and telecommunications network around the world, under the sea, and in the air is subject to proprietary interests—whether that of a private company, a sovereign government, or possibly both.¹¹ Each copper wire, fiber-optic cable, microwave relay tower, satellite transponder, or Internet router has been produced or installed by some entity whose legal successors not only maintain ownership of that physical asset but also expect protection of the same by

7. See, e.g., Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEXAS L. REV. 553, 556–57 (1998) (recounting a specific attempt to control pornography on the Internet and the subsequent holding by the U.S. Supreme Court that the law was unconstitutional).

8. See, e.g., Anne Flanagan, *The Law and Computer Crime: Reading the Script of Reform*, 13 INT'L J.L. & INFO. TECH. 98, 109 (2005) (discussing the Council of Europe's promulgation of an international treaty addressing computing and crime as well as a law subsequently passed in the United Kingdom based on the treaty).

9. See, e.g., INTERPOL, Secure Global Police Communications Services, <http://www.interpol.int/Public/ICPO/corefunctions/securecom.asp> (“INTERPOL developed the I-24/7 global police communications system . . . creating a global network for the exchange of police information and providing law enforcement authorities in member countries with instant access to the organization's databases and other services.”).

10. See U.N. Charter art. 2, para. 1 (“The Organisation is based on the principle of the sovereign equality of all its Members.”).

11. See, e.g., *T-Mobile West Corp. v. Crow*, No. CV08-1337-PHX-NVW, 2009 WL 5128562, at *15–16 (D. Ariz. Dec. 17, 2009) (discussing the proprietary interest in wireless telecommunications systems); *Med. Informatics Eng'g v. Orthopaedics Ne.*, No. 1:06-CV-173, 2008 WL 4099110, at *6 (N.D. Ind. Sept. 2, 2008) (assuming, without discussion, the existence of proprietary interests in computer software).

sovereign authorities.¹² When those infrastructure elements are emplaced within the terrestrial boundaries, territorial waters, or exclusive airspace of a nation-state, it can exert its sovereign authority over them.¹³ Just as with other transnational legal matters, governments may also try to invoke extra-territorial jurisdiction in order to defend the property rights of their nationals' interests.

Even though the ether itself may not be owned per se, legal strictures can be imposed on the means by which wireless communications and media broadcasts are propagated through that medium. National regulations as well as those established under the auspices of the International Telecommunication Union (ITU) allocate electromagnetic frequencies among potential users and proscribe unauthorized interference.¹⁴ Cuba, for example, has repeatedly argued that unauthorized foreign radio and television broadcasts into its territory violate both its national sovereignty and the explicit provisions of international conventions.¹⁵

In addition to defending physical assets or restricting use of the electromagnetic spectrum, multiple governments have sought to regulate their nations' information spaces by delimiting what content should or should not be made available to their populace even through approved channels. Foreign courts have ordered American Internet service providers to filter certain material from their European Web sites.¹⁶ The member states of the

12. See *supra* note 11 and accompanying text.

13. See ANTONIO CASSESE, *INTERNATIONAL LAW* 81 (2d ed. 2005) (“[W]hoever had the physical means of acquiring and effectively controlling a portion of territory on land was legitimized to claim sovereign rights over it.”).

14. For example, the Constitution of the ITU states,

All stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States or of recognized operating agencies, or of other duly authorized operating agencies which carry on a radio service, and which operate in accordance with the provisions of the Radio Regulations.

CONSTITUTION OF THE INTERNATIONAL TELECOMMUNICATION UNION art. 45(1) [hereinafter ITU CONSTITUTION].

15. See The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 8, delivered to the General Assembly, U.N. Doc. A/64/129/Add.1 (Sept. 9, 2009) (claiming that even a U.S. General Accounting Office report from January 2009 “recognizes the violations of international norms and domestic legislation incurred by the programme of radio and television broadcasts by the United States Government against Cuba”).

16. See Edmund L. Andrews, *German Court Overturns Pornography Ruling Against Compuserve*, N.Y. TIMES, Nov. 18, 1999, at C4 (discussing the prosecution, conviction, and subsequent acquittal on appeal of Compuserve Deutschland executive Felix Somm for failure to filter objectionable material hosted by Compuserve’s parent company, a U.S.-based Internet service provider). In May 2000, a French court also sought to impose content limitations on a U.S.-based Internet service provider when it ruled, “We order the Company YAHOO! Inc. to take all necessary measures to dissuade and render impossible any access via Yahoo.com to the Nazi artifact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes.” *Yahoo!, Inc. v. La Ligue Contre le Racisme et L’antisémitisme*,

Shanghai Cooperation Organization (SCO)—China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan—have also offered justifications for sovereign controls on informational content in their regional treaty.¹⁷ China and Qatar have each maintained that “the free flow of information should be guaranteed under the premises that national sovereignty and security must be safeguarded”¹⁸ and that “each country has the right to manage its own cyberspace in accordance with its domestic legislation.”¹⁹

Both the infrastructure and content of cyberspace remain subject to national jurisdiction in the eyes of most sovereigns,²⁰ thereby making effective regulation a question of legal and technical implementation rather than one of right. Once one appreciates that governments seek to extend their sovereign authority into this new realm, it then becomes necessary to analyze how their interests may align or conflict in regard to nonexclusive resources.

B. *Misnomer of a Global Commons*

Cyberspace has become a critical feature of modern society that manifests the profound interdependencies of all nations. As a result, some commentators are considering whether this new realm should be considered a “global commons” and governed collectively for the common benefit of all mankind (including sovereign states, private companies, individuals, etc.). While the notion of a global commons is not always interpreted consistently, it stems from the two disciplines of international law and political

169 F. Supp. 2d 1181, 1185 (N.D. Cal. 2001) (quoting the translation of an order by the High Court of Paris), *rev'd*, 433 F.3d 1199 (9th Cir. 2006).

17. Among the “main threats in the field of ensuring international information security” listed in that treaty is “[d]issemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other States.” Agreement Between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security art. 2, June 16, 2009 [hereinafter SCO Agreement], *unofficial translation in* INTERNATIONAL INFORMATION SECURITY: THE DIPLOMACY OF PEACE: COMPILATION OF PUBLICATIONS AND DOCUMENTS 202, 203 (Moscow 2009).

18. The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 7, *delivered to the General Assembly*, U.N. Doc. A/62/98 (July 2, 2007).

19. The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 4, *delivered to the General Assembly*, U.N. Doc. A/61/161 (July 18, 2006). For Qatar’s official submission to the U.N. Secretary-General, see The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 8, *delivered to the General Assembly*, U.N. Doc. A/63/139 (July 18, 2008) (repeating the relevant portions of the two earlier Chinese submissions almost verbatim).

20. See Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 FED. COMM. L.J. 117, 129–44 (1997) (applying bases of national jurisdiction, namely the territoriality, nationality, effects, protective, and universality principles, to cyberspace).

economy.²¹ In order to ascertain the extent to which cyberspace should (or could effectively) be coordinated as a global commons, one must first understand both the treaty frameworks applied to other so-called commons (e.g., the high seas, outer space, and Antarctica²²) and the logical criteria that must exist to warrant specialized institutions (such as collective agreements and cultural norms) that ensure communal access to particular resources.

Regarding international legal commons, it is noteworthy that in every case mankind came to those pre-existing regions through discovery; since people had no part in their creation or development, legacy property interests were not of concern. The resulting international agreements specified certain portions of the oceans and airspace as commons (for instance, the high seas beyond 200 nautical miles and outer space above an altitude of approximately 100 kilometers), but they also retained principles of sovereignty regarding both the "territory" within or below those limits and the vessels that ventured into the genuinely common areas of those realms for exploration, commerce, and recreation. Moreover, international law has also developed complex governance mechanisms for the allocation and use of certain key natural resources—such as fisheries, geostationary orbits, and electromagnetic frequencies—within the agreed common areas.²³

There are two critical considerations when comparing and contrasting cyberspace to existing legal commons. First, the medium itself, while

21. For an introduction to the notion of commons under international law, see generally IAN BROWNLIE, *PRINCIPLES OF PUBLIC INTERNATIONAL LAW* 249–73 (7th ed. 2008) and CASSESE, *supra* note 13, at 81–97. For an introduction to the notion of commons under political economy, see generally ELINOR OSTROM, *GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION* (1990).

22. To understand similar agreements relating to other commons, see, for example, United Nations Convention on the Law of the Sea, pt. VII, Dec. 10, 1982, 1833 U.N.T.S. 3 [hereinafter *Law of the Sea*] (governing the high seas); Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, *adopted* Dec. 5, 1979, 1363 U.N.T.S. 3 (covering outer space); Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, *opened for signature* Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 (governing outer space); and Antarctic Treaty, Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 71 (covering Antarctica).

23. In regard to fisheries, see, for example, Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 Relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks, *opened for signature* Dec. 4, 1995, S. TREATY DOC. NO. 104-24 (1996), 2167 U.N.T.S. 3 (regulating fisheries in order to promote conservation of migratory and straddling fish stocks) and Convention on Future Multilateral Co-operation in North-East Atlantic Fisheries, Nov. 18, 1980, 1285 U.N.T.S.

129. ITU regulations apply to the use of geostationary orbits and electromagnetic frequencies:

In using frequency bands for radio services, Member States shall bear in mind that radio frequencies and any associated orbits, including the geostationary-satellite orbit, are limited natural resources and that they must be used rationally, efficiently and economically, in conformity with the provisions of the Radio Regulations, so that countries or groups of countries may have equitable access to those orbits and frequencies, taking into account the special needs of the developing countries and the geographical situation of particular countries.

ITU CONSTITUTION, *supra* note 14, art. 44(2).

subject to the natural laws of physics, has in essence been generated by mankind. Second, even the recognized commons are not treated as such in their entirety. Instead of merely choosing to establish a commons in lieu of adjudicating competing claims of discovery, any legal arbiter of cyberspace would need to override the long-established rights of sovereignty and property ownership recognized by the numerous domestic jurisdictions involved.²⁴ In addition, well-reasoned and equitable decisions would need to be reached regarding how much, and which specific portions, of cyberspace would be subjected to collective governance.

For example, one can imagine that most nation-states would be adverse to declaring the dedicated information and communication technology networks upon which their government and security apparatuses rely as common resources; yet many of those same nations would also oppose the refusal of any nation to permit its citizenry to enter the "high seas" of cyberspace to exchange ideas and conduct international trade. If sovereignty or property rights are to be recognized for certain portions or applications of cyberspace, then international customs and norms of behavior will have to be agreed upon for transit through or operation within those infrastructure elements rightfully owned by others.²⁵

But even before one could attempt to develop cooperative rules for a newly ordained global commons of cyberspace, one would first have to determine if the logical circumstances of the situation warranted such a designation and those concomitant efforts. As decades of academic study have shown, not all resource systems either (a) experience the sort of collective action problems that require open access and communal governance for efficient, sustainable operation or (b) lend themselves to the particular solution embodied in the designation of a commons.²⁶ The basic principle behind governing the commons for political economists is the need to prevent the overexploitation of resources where no individual actor has the incentive structure necessary to pay the cost of providing a collective good or to constrain his actions in the ways necessary to preserve the future availability of a common resource.²⁷

24. See *supra* notes 11–13 and accompanying text.

25. Imperfect but useful analogies exist to inform this process, including nonexclusive rights of innocent passage through territorial waters and responsibility for incidental damage to foreign satellites. See, e.g., Law of the Sea, *supra* note 22, arts. 17–32 (governing the right of innocent passage in territorial seas); Convention on the International Liability for Damage Caused by Space Objects, *opened for signature* Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187 (setting forth liability requirements for damage caused by space objects).

26. For a summary of the required conditions to achieve a sustainable commons see OSTROM, *supra* note 21, at 90 tbl.3.1, 211. For qualitative analyses of public resources and the necessary conditions to overcome collective action problems, see generally RUSSELL HARDIN, *COLLECTIVE ACTION* (1982) and MANCUR OLSON JR., *THE LOGIC OF COLLECTIVE ACTION* (rev. ed. 1971).

27. See Garrett Hardin, *The Tragedy of the Commons*, 162 *SCI.* 1243, 1244 (1968) ("Ruin is the destination toward which all men rush, each pursuing his own best interest in a society that believes in the freedom of the commons.").

The aggregate effect of that unfortunate microeconomic reality is often referred to as the “tragedy of the commons.”²⁸ Whether one analyzes communal grazing meadows in Alpine, Switzerland,²⁹ or fishing limitations under relevant conventions,³⁰ the same principle maintains. That principle also implies that the notion of a commons which requires collective management will not exist regarding a truly public good (i.e., a resource whose value and availability are not degraded or diminished by other individuals’ use of that same resource).³¹

Additional conditions of a true commons are that the affected individuals have insufficient incentives to make investments to properly manage their resources and that a sustainable solution is only possible if reliable mechanisms are established to enforce compliance.³² It remains uncertain if market forces, or other regulatory options, are capable of providing adequate incentives in cyberspace because technical factors limit reliable identity management, attribution, and deterrence.³³ Cooperative enforcement cannot be fully achieved in cyberspace given the current status of forensic technologies and the incomplete transnational judicial cooperation in many such investigations.³⁴ In marked contrast, according to the maritime

28. *Id.* at 1243.

29. OSTROM, *supra* note 21, at 62–64 (describing the controls that have prevented overgrazing in Swiss villages).

30. *See, e.g.*, Convention on Future Multilateral Co-operation in North-East Atlantic Fisheries, *supra* note 23 (establishing a commission to help regulate fisheries in the North-East Atlantic).

31. *See* HARDIN, *supra* note 26, at 17 (“Public goods are defined by two properties: *jointness of supply* and *impossibility of exclusion*.”); OLSON, *supra* note 26, at 14 (“A common, collective, or public good is here defined as any good such that, if any person X_i in a group $X_1, \dots, X_i, \dots, X_n$ consumes it, it cannot feasibly be withheld from the others in that group.”).

32. *See* Daniel Fitzpatrick, *Evolution and Chaos in Property Rights Systems: The Third World Tragedy of Contested Access*, 115 YALE L.J. 996, 1001 n.15 (2006) (“A tragedy of the commons arises when insufficient incentives exist for resource conservation and investment in productive capacity, because no user bears all the costs and consequences of his resource use.”); Kevin Werbach, *Supercommons: Toward a Unified Theory of Wireless Communication*, 82 TEXAS L. REV. 863, 936–37 (2004) (explaining that every commons does not lead to a tragedy when there are rules and enforcement mechanisms to preserve public character).

33. The inherent difficulty of positively identifying actors in cyberspace and definitively attributing actions to them undermines the basic requirements of a collective action system. As one of her key design principles for successful common-pool resource (CPR) institutions, Nobel laureate Elinor Ostrom has argued that “[i]ndividuals or households who have rights to withdraw resource units from the CPR must be clearly defined, as must the boundaries of the CPR itself.” OSTROM, *supra* note 21, at 91. “Furthermore, the long-term sustainability of rules devised at a focal SES [social-ecological system] level depends on monitoring and enforcement as well their not being overruled by larger government policies.” Elinor Ostrom, *A Generalized Framework for Analyzing Sustainability of Social-Ecological Systems*, 325 SCI. 419, 422 (2009).

34. *See* Andrew Jacobs, *E-mail Accounts of Activists, Scholars and Journalists Hit by Hackers in China*, N.Y. TIMES, Mar. 31, 2010, at A8 (“[E]xperts point out that attacks appearing to come from a certain location can just as easily be emanating from computers infected with botnets, a virus that allows them [to] be controlled remotely by other computing systems.”); John Markoff & David Barboza, *Academic Paper in China Sets Off Alarms in U.S.*, N.Y. TIMES, Mar. 21, 2010, at A10 (discussing the charged atmosphere between the United States and China concerning cybersecurity issues and how difficult it is to respond to incidents because “it is so easy to mask the true source of

model originally instituted under the traditional “law of nations” (the analogue of modern customary international law and the intellectual precursor of codified treaties such as the Law of the Sea), the navies of all sovereign states were empowered to enforce the agreed principles, and in fact, the crime of piracy on the high seas became one of the first peremptory norms subject to universal jurisdiction.³⁵

From the political-economy perspective, then, cyberspace in its extant form fails to satisfy two logical criteria for successful treatment as a commons since (i) the underlying physical resources remain subject to private property rights and (ii) the positive identification of legitimate users—as well as the exclusion of illegitimate users—is not yet possible (thereby preventing enforcement of any established norms or collective solutions). One must also consider the economic implications of designating a global commons. History has shown that such systems lack adequate investment and innovation since no single entity can reap the full benefit of its own contributions.³⁶ They operate best where no maintenance of the medium is required (for instance, naturally occurring realms such as the ocean or outer space) or where the resource will naturally replenish itself—provided that it is not overutilized to the point of exhaustion (e.g., pastures, forests, and fisheries).³⁷

Despite the uncertain applicability of either the international law or political-economy conception of a commons to cyberspace, some lessons can still be learned from existing legal frameworks and potentially applied to this new realm. Perhaps one of the most pertinent legal regimes concerns the polar archipelago of Svalbard (also known as Spitsbergen), where economic and ecological resources have been designated for the common benefit of multiple nations.³⁸ Although Norway bears the legal responsibility and cost

a computer network attack”); CYBER SEC. STRATEGY COMM., ESTONIAN MINISTRY OF DEF., CYBER SECURITY STRATEGY 17 (2008), http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strategie_2008-2013_ENG.pdf [hereinafter ESTONIAN CYBERSECURITY STRATEGY] (“Since every country can decide for itself whether to co-operate in criminal procedures dealing with cyber attacks, legal solutions for the protection of cyberspace serve their purpose only when implemented in individual countries or when co-operation with other countries on an *ad hoc* basis is possible.”); PAUL ROSENZWEIG, AM. BAR ASS’N STANDING COMM. ON LAW & NAT’L SEC., NATIONAL SECURITY THREATS IN CYBERSPACE 2 (2009), http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf (asserting that because “the nature of cyberspace is such that we currently lack the technical capacity to attribute actions to the responsible actors with a high degree of confidence[,] . . . practical anonymity is achievable”).

35. See Bradford R. Clark, *Federal Common Law: A Structural Reinterpretation*, 144 U. PA. L. REV. 1245, 1280 & n.168 (1996) (describing the law maritime as one of the historical branches of the “law of nations”); Kenneth C. Randall, *Universal Jurisdiction Under International Law*, 66 TEXAS L. REV. 785, 791 (1988) (“Piracy is the oldest offense that invokes universal jurisdiction.”).

36. See Ostrom, *supra* note 33, at 420 (explaining how the increased cost of managing a large resource system undermines the incentive to self-regulate).

37. See *id.* at 419–20 (arguing that resource systems that require lower governance costs can avoid overutilization and destruction).

38. According to the international agreement regarding that archipelago, The nationals of all the High Contracting Parties shall have equal liberty of access and entry for any reason or object what[so]ever to the waters, fjords, and ports of

of administering most of the islands' territory, its sovereignty is incomplete and serves largely to preserve those resources in accordance with foreign interests (i.e., right of access for other nations and equal opportunity for economic and scientific activities).³⁹ This arrangement begins to resemble a trusteeship more than ownership and may represent a feasible alternative to current measures for Internet governance. A second legal paradigm for analogical consideration would be the system that governs international waterways (i.e., inland rivers, straits, and lakes with common rights of access). In this case, although adjacent countries maintain certain sovereign rights, their control is not absolute and must be balanced with the interests of their riparian neighbors as well as international navigation.⁴⁰

Considering (or declaring) cyberspace to be a global commons would require the partial subordination of sovereignty and established property rights in numerous jurisdictions. Neither the sea nor airspace is treated as a commons in its entirety.⁴¹ Likewise, any collective governance structure for cyberspace would also require careful distinction between possessory assets and the true commons. Finally, scholarship in political economy has shown that commons are often prone to collective action problems that encourage misuse while also discouraging investment and innovation. All of these factors will need to be weighed as new strategic and legal paradigms are considered for cyberspace.

III. International Norms

A. *Dialogue on Cybersecurity*

Thus far, international engagement and cooperation on rules in cyberspace can be divided into three categories: Internet governance, multilateral public policy, and international security.⁴² As used herein, the

the territories specified in Article 1; subject to the observance of local laws and regulations, they may carry on there without impediment all maritime, industrial, mining and commercial operations on a footing of absolute equality.

Treaty Concerning the Archipelago of Spitsbergen, art. 3, Feb. 9, 1920, 43 Stat. 1892, 2 L.N.T.S. 7.

39. *Id.* art. 1 ("The High Contracting parties undertake to recognise, *subject to the stipulations of the present Treaty*, the full and absolute sovereignty of Norway over the Archipelago of Spitsbergen . . .") (emphasis added).

40. See BROWNIE, *supra* note 21, at 261–63 (presenting various formulations of international law that account for riparian interests).

41. See *id.* at 115–16 (explaining that because airspace is appurtenant to territorial land and water, there are constraints on the free navigation of airspace that mirror constraints on the free navigation of international waters).

42. Each of those different subjects is being discussed in numerous forums as various governments seek venues that are most conducive to their own policy interests. According to the White House,

More than a dozen international organizations—including the United Nations, the Group of Eight, NATO, the Council of Europe, the Asia-Pacific Economic Cooperation forum, the Organization of American States, the Organization of Economic Cooperation and Development, the International Telecommunication

term “Internet governance” refers to the organization, standardization, and technical administration of the Internet’s infrastructure.⁴³ The second rubric of multilateral public policy is meant to describe legal issues that would ordinarily be of domestic concern, except that the interconnected nature of the global information and communication technology (ICT) infrastructure gives them a new transnational dimension.

Those topics include cross-border law enforcement cooperation against cybercrime, the harmonization of data privacy regulations, and the protection of fundamental human rights and civil liberties.⁴⁴ Among the most notable international documents to date in this area are the Council of Europe (COE) Convention on Cybercrime⁴⁵ and five U.N. General Assembly (UNGA) resolutions⁴⁶ from its Second and Third Committees regarding the “creation of a global culture of cybersecurity”⁴⁷ and “combating the criminal misuse of information technologies,”⁴⁸ respectively.

While each and every one of the topics already mentioned in this section warrants concerted international attention, the remainder of this Article will focus on the third and final category, namely sovereign discourse on international security and arms control in cyberspace.

The potential for military activities in cyberspace raises national security concerns that some states are now seeking to allay through multilateral agreements.⁴⁹ Since 1998, the UNGA First Committee—whose

Union (ITU), and the International Organization for Standardization (ISO)—address issues concerning the information and communications infrastructure.

WHITE HOUSE, *supra* note 3, at 20.

43. For a detailed discussion of governmental involvement in those processes and the multiplicity of international organizations related thereto, see Harold Kwalwasser, *Internet Governance*, in *CYBERPOWER AND NATIONAL SECURITY* 491 (Franklin D. Kramer et al. eds., 2009). That chapter summarizes the roles of, *inter alia*, the Domain Name System (DNS), Internet Corporation for Assigned Names and Numbers (ICANN), Internet Assigned Numbers Authority (IANA), Internet Governance Forum (IGF), Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE), International Telecommunication Union (ITU), International Organization for Standardization (ISO), and World Wide Web Consortium in the organization and administration of the Internet.

44. See WHITE HOUSE, *supra* note 3, at 20 (“[D]iffering national and regional laws and practices—such as those laws concerning the investigation and prosecution of cybercrime; data preservation, protection, and privacy; and approaches for network defense and response to cyber attacks—present serious challenges to achieving a safe, secure, and resilient digital environment.”).

45. Council of Europe, Convention on Cybercrime, *opened for signature* Nov. 11, 2001, Europ. T.S. No. 185.

46. G.A. Res. 64/211, U.N. Doc. A/RES/64/211 (Dec. 21, 2009); G.A. Res. 58/199, U.N. Doc. A/RES/58/199 (Dec. 23, 2003); G.A. Res. 57/239, U.N. Doc. A/RES/57/239 (Dec. 20, 2002); G.A. Res. 56/121, U.N. Doc. A/RES/56/121 (Dec. 19, 2001); G.A. Res. 55/63, U.N. Doc. A/RES/55/63 (Dec. 4, 2000).

47. G.A. Res. 64/211, U.N. Doc. A/RES/64/211 (Dec. 21, 2009).

48. G.A. Res. 57/239, U.N. Doc. A/RES/57/239 (Dec. 20, 2002).

49. See generally SCO Agreement, *supra* note 17 (setting forth the terms of an agreement governing cooperation in international information security between China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan); MCAFEE, INC., VIRTUAL CRIMINOLOGY REPORT

mandate covers international security and disarmament affairs—has annually passed a resolution entitled “Developments in the field of information and telecommunications in the context of international security” that invites U.N. member states to provide their official views on international information security to the U.N. Secretary-General.⁵⁰ But each of the seventy-eight responses submitted by a total of forty-two countries through 2009 remains just that—the expression of a national viewpoint which carries no controlling authority beyond its own borders, although it might play a contributory role in the formation of customary international law over time.⁵¹ Pursuant to

13 (2009), http://img.en25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf (identifying several countries that are developing cyber-warfare capabilities).

50. G.A. Res. 64/25, U.N. Doc. A/RES/64/25 (Dec. 2, 2009); G.A. Res. 63/37, U.N. Doc. A/RES/63/37 (Dec. 2, 2008); G.A. Res. 62/17, U.N. Doc. A/RES/62/17 (Dec. 5, 2007); G.A. Res. 61/54, U.N. Doc. A/RES/61/54 (Dec. 6, 2006); G.A. Res. 60/45, U.N. Doc. A/RES/60/45 (Dec. 8, 2005); G.A. Res. 59/61, U.N. Doc. A/RES/59/61 (Dec. 3, 2004); G.A. Res. 58/32, U.N. Doc. A/RES/58/32 (Dec. 8, 2003); G.A. Res. 57/53, U.N. Doc. A/RES/57/53 (Nov. 22, 2002); G.A. Res. 56/19, U.N. Doc. A/RES/56/19 (Nov. 29, 2001); G.A. Res. 55/28, U.N. Doc. A/RES/55/28 (Nov. 20, 2000); G.A. Res. 54/49, U.N. Doc. A/RES/54/49 (Dec. 1, 1999); G.A. Res. 53/70, U.N. Doc. A/RES/53/70 (Dec. 4, 1998).

51. See The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/64/129/Add.1 (Sept. 9, 2009) [hereinafter *Developments in the Field Add.* (Sept. 9, 2009)]; The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/64/129 (July 8, 2009) [hereinafter *Developments in the Field* (July 8, 2009)]; The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/63/139 (July 18, 2008); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/62/98/Add.1 (Sept. 17, 2007); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/62/98 (July 2, 2007); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/61/161/Add.1 (Oct. 31, 2006); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/61/161 (July 18, 2006); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/60/95/Add.1 (Sept. 21, 2005); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/60/95 (July 5, 2005); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/59/116/Add.1 (Dec. 28, 2004) [hereinafter *Developments in the Field Add.* (Dec. 28, 2004)]; The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/59/116 (June 23, 2004) [hereinafter *Developments in the Field* (June 23, 2004)]; The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/58/373 (Sept. 17, 2003); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/57/166/Add.1 (Aug. 29, 2002); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, delivered to the General Assembly, U.N. Doc. A/57/166 (July 2, 2002); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of*

those UNGA resolutions from 2005 through 2009, a second U.N. group of governmental experts has been convened during 2009–2010 to consider international information security.⁵²

The U.N. Institute for Disarmament Research sponsored meetings in 1999 and 2008 to further explore international information security⁵³ and even dedicated an issue of its quarterly journal to this topic in 2007.⁵⁴ Several regional organizations—such as the SCO, the North Atlantic Treaty Organization (NATO), and the Organization for Security and Cooperation in Europe (OSCE)—have also begun dialogues on legal measures to ensure international information security and respond to cyber attacks.⁵⁵ Although many of these U.N. and regional initiatives have not yielded concrete results

International Security, delivered to the General Assembly, U.N. Doc. A/56/164/Add.1 (Oct. 3, 2001); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/56/164 (July 3, 2001) [hereinafter *Developments in the Field* (July 3, 2001)]; The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/55/140/Add.1 (Oct. 3, 2000); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/55/140 (July 10, 2000); The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly*, U.N. Doc. A/54/213 (Aug. 10, 1999) (providing various state contributions to the Secretary-General).

52. G.A. Res. 64/25, ¶ 4, U.N. Doc. A/RES/64/25 (Dec. 2, 2009); G.A. Res. 63/37, ¶ 4, U.N. Doc. A/RES/63/37 (Dec. 2, 2008); G.A. Res. 62/17, ¶ 4, U.N. Doc. A/RES/62/17 (Dec. 5, 2007); G.A. Res. 61/54, ¶ 4, U.N. Doc. A/RES/61/54 (Dec. 6, 2006); G.A. Res. 60/45, ¶ 4, U.N. Doc. A/RES/60/45 (Dec. 8, 2005). In 2009, the U.N. Secretary-General's Advisory Board on Disarmament Affairs was also tasked to study the issue of "cyber warfare and its impact on international security." Sergio Duarte, U.N. High Representative for Disarmament Affairs, Opening Remarks to the Advisory Board on Disarmament Matters (Feb. 18, 2009), available at <http://www.pfcmc.com/disarmament/HomePage/HR/docs/2009Feb18HRTtoABDM.pdf>; accord Ban Ki-moon, U.N. Sec'y-Gen., Remarks to the Advisory Board on Disarmament Matters (Feb. 18, 2009), available at <http://www.unrcpd.org.np/uploads/library/file/Statement%20cyberwarfare.pdf>.

53. Conference, *Information & Communications Technologies and International Security*, U.N. INST. FOR DISARMAMENT RES. (April 24–25, 2008), audio available at http://www.unidir.org/audio/2008/Information_Security/en.htm; Private Discussion Meeting, *Developments in the Field of Information and Telecommunications in the Context of International Security*, DEP'T OF DISARMAMENT AFF. & U.N. INST. FOR DISARMAMENT RES. (Aug. 25–26, 1999).

54. Colloquy, *ICTs and International Security*, DISARMAMENT F., 2007 (Issue 3).

55. See SCO Agreement, *supra* note 17 (memorializing the terms of the agreement regarding cooperation in international information security between members of the SCO); Vladislav Sherstyuk, Deputy Dir., Sec. Council of the Russian Fed'n, Keynote Presentation at Working Session I of the OSCE Workshop on a Comprehensive OSCE Approach to Enhancing Cyber Security (Mar. 18, 2009) (translated transcript on file with Texas Law Review) (advocating new legal measures to combat hostile uses of information and communications technology); James Stavridis, NATO Supreme Allied Commander Eur., SACEUR Address to the Armed Forces Communications and Electronics Association (Feb. 2, 2010), available at <http://www.aco.nato.int/page27750625.aspx?print=y> (proposing that NATO's reciprocal protection for members be extended to include cyber attacks). The NATO-accredited Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, has also organized professional conferences on this topic. See, e.g., Press Release, Coop. Cyber Def. Ctr. of Excellence, President of Estonia opened International Cyber Conflict Legal and Policy Conference (Sept. 9, 2009), <http://www.ccdcoe.org/149.html> ("[W]e are making our way to tackle the bottlenecks in cyber conflict legal and policy areas.").

yet (with the SCO being a notable exception⁵⁶), it is clear that the international community sees cyber conflict between sovereign nations as a growing concern worthy of increased legal attention.

B. Sources of Customary International Law

Public international law represents an amalgam of different legal systems that also contains its own unique elements. The Statute of the International Court of Justice (ICJ)—a treaty to which all U.N. members are party *ipso facto* by its incorporation into the U.N. Charter⁵⁷—lists the appropriate sources of international law that the ICJ may rely upon in rendering its decisions.⁵⁸ Notable among those sources are “international custom, as evidence of a general practice accepted as law” and “the general principles of law recognized by civilized nations,” which together form the basis of customary international law.⁵⁹ The Statute of the International Law Commission (ILC)—the U.N. organ tasked with codifying and promulgating international law—provides further guidance on the sources of customary international law.⁶⁰ Article 19 of that Statute directs the ILC to obtain “texts of laws, decrees, judicial decisions, treaties, diplomatic correspondence and other documents relevant to the topic being studied” from the governments of U.N. member states.⁶¹ Similarly, Article 20 calls for “[a]dequate presentation of precedents and other relevant data, including treaties, judicial

56. See Pan Guang, *The SCO's Success in Security Architecture* (highlighting confidence building, cooperation against destabilizing transborder elements, and the maintenance of regional security and stability as general successes of the SCO), in *THE ARCHITECTURE OF SECURITY IN THE ASIA-PACIFIC* 33, 33–34 (Ron Huiskens ed., 2009).

57. U.N. Charter arts. 92–93.

58. Statute of the International Court of Justice art. 38(1), June 26, 1945, 59 Stat. 1055, 1060, T.S. No. 993 [hereinafter ICJ Statute]. According to the ICJ Statute,

The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:

- (a) international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;
- (b) international custom, as evidence of a general practice accepted as law;
- (c) the general principles of law recognized by civilized nations;
- (d) subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

Id.

59. *Id.*

60. Pursuant to its authorities under the U.N. Charter, the UNGA has resolved that “[t]he International Law Commission shall have for its object the promotion of the progressive development of international law and its codification.” G.A. Res. 174 (II), art. 1(1), U.N. Doc. A/519 (Nov. 21, 1947) [hereinafter ILC Statute]. “[T]he expression ‘codification of international law’ is used for convenience as meaning the more precise formulation and systematization of rules of international law in fields where there already has been extensive state practice, precedent and doctrine.” *Id.* art. 15.

61. *Id.* art. 19(2).

decisions and doctrine.”⁶² Since both the ICJ and ILC Statutes clearly indicate state practice to be a legitimate—and guiding—source of customary international law, they confirm that what sovereign governments do and say directly affects the law itself.⁶³

Nothing could be more critical in the context of cyberspace; for in the absence of historical precedents and codified rules, new international norms are being created by those government officials who are rendering legal opinions, declaring national security policies, formulating military doctrines, establishing rules of engagement, and otherwise providing evidence of state practice. Moreover, state actors seeking national advantage through cyber conflict have the opportunity to resist multilateral constraints by both rejecting treaty mechanisms and also taking certain military actions that would set precedents for the future. Conversely, multilateral efforts—such as the impending report from the current U.N. group of governmental experts—could serve to establish some norms of behavior in cyberspace that would delineate what is not acceptable to the international legal community. Perhaps there will be an international cyber-arms-control instrument in the future, but that seems unlikely in the near term. Until then, state practice remains the primary source of customary international law on this topic.

C. *State Practice in Cyberspace*

The modern rules of *ius ad bellum*, or the principles of just war, are derived from the U.N. Charter. Although one can easily locate references to “acts of aggression,”⁶⁴ “the threat or use of force,”⁶⁵ and “armed attack,”⁶⁶ those terms all remain undefined in the Charter itself. “The difficulties are exacerbated by the absence of any generally accepted interpretations of [those] concepts . . . in relation to information security.”⁶⁷ Even though other nonbinding sources of “soft law” have attempted to clarify those terms,⁶⁸

62. *Id.* art. 20(a).

63. As a “means for making the evidence of customary international law more readily available,” the ILC is explicitly tasked to collect and publish “documents concerning State practice and of the decisions of national and international courts on questions of international law.” *Id.* art. 24. For additional discussion of state practice and related sources of customary international law, see Ways and Means for Making the Evidence of Customary International Law More Readily Available, in Report of the International Law Commission Covering Its Second Session ¶¶ 24–94, U.N. GAOR, 5th Sess., Supp. No. 12, at 4–10, U.N. Doc. A/1316 (1950).

64. U.N. Charter art. 1, para. 1.

65. *Id.* art. 2, para. 4.

66. *Id.* art. 51.

67. *Developments in the Field Add.* (Sept. 9, 2009), *supra* note 51, at 7; see also Streltsov, *supra* note 4, at 9 (providing a nearly verbatim assessment of the definitional and interpretative problems); ESTONIAN CYBER SECURITY STRATEGY, *supra* note 34, at 17 (“Several terms, such as *cyber warfare*, *cyber attack*, *cyber terrorism*, or *critical information infrastructure*, have not been defined clearly. Everywhere they are used, but their precise and intended meaning will vary depending on the context.”).

68. See, e.g., G.A. Res. 3314 (XXIX), Annex art. 1, U.N. Doc. A/9631 (Dec. 14, 1974) (“Aggression is the use of armed force by a State against the sovereignty, territorial integrity or

sovereign governments actively seek to influence the legal interpretations of those provisions when they formulate national security strategies and issue declaratory policy statements. Mali, for instance, has claimed,

The use of an information weapon could be interpreted as an act of aggression if the victim State has reasons to believe that the attack was carried out by the armed forces of another State and was aimed at disrupting the operation of military facilities, destroying defensive and economic capacity, or violating the State's sovereignty over a particular territory.⁶⁹

The United States and Russia have both made pronouncements that cyber conflicts could have significant impacts on national security and that they will take necessary measures to protect their information infrastructures.⁷⁰ Each of those countries plays a leading role in world affairs—*inter alia* as permanent members of the U.N. Security Council—so how they decide to “deter, prevent, detect, and defend against” cyber attacks and “recover quickly from any disruptions or damage” will set a precedent for the rest of the world.⁷¹ Their state practice in developing military capabilities for cyberspace⁷² will also serve as a model for others. As one

political independence of another State, or in any other manner inconsistent with the Charter of the United Nations . . .”).

69. *Developments in the Field Add.* (Sept. 9, 2009), *supra* note 51, at 8.

70. President Barack Obama declared, “From now on, our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority.” Barack Obama, U.S. President, Remarks on Securing Our Nation’s Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure. Similarly, Russia has stated, “The information weapon is particularly dangerous when used against military and civilian buildings and State systems and institutions, the disruption of the normal functioning of which constitutes a direct threat to national security.” The Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 2, delivered to the General Assembly, U.N. Doc. A/56/164/Add.1 (Oct. 3, 2009); see also Doctrine of the Information Security of the Russian Federation art. 1, approved June 23, 2000 [hereinafter Russian Information Security Doctrine] (“The national security of the Russian Federation depends to a substantial degree on ensuring the information security, a dependence that will increase with technological progress.”), reprinted in *RUSSIAN MEDIA LAW AND POLICY IN THE YELTSIN DECADE* 492 (Monroe E. Price et al. eds., 2002).

71. Obama, *supra* note 70.

72. According to one U.S. military leader,

In this emerging war-fighting domain, USSTRATCOM, through the Joint Task Force for Global Network Operations (JTF-GNO) and the Joint Functional Component Command for Network Warfare (JFCC-NW), in partnership with the Joint Staff is leading the planning and execution of the National Military Strategy for Cyberspace Operations. In this role, we coordinate and execute operations to defend the Global Information Grid (GIG) and project power in support of national interests.

United States Strategic Command: Hearing Before the Strategic Forces Subcomm. of the H. Armed Servs. Comm., 110th Cong. (2008) (statement of Gen. Kevin P. Chilton, Commander, U.S. Strategic Command), available at http://armedservices.house.gov/pdfs/STRAT022708/Chilton_Testimony022708.pdf; see also Military Doctrine of the Russian Federation ¶ 41(c), Feb. 5, 2010, unofficial translation available at http://merln.ndu.edu/whitepapers/Russia2010_English.pdf

member of the Russian delegation to the U.N. group of governmental experts on international information security has written, "There is no doubt that information weapons can be used in practice. Some armed forces are already preparing special units for military operations using ICTs."⁷³

A similar process of state practice informing customary international law is also underway regarding the rules of *jus in bello* that comprise international humanitarian law (IHL), also known as the law of armed conflict. Although the Geneva Conventions and other treaty instruments have endeavored to codify general principles for the conduct of armed conflicts (including necessity, proportionality, distinction, discrimination, and humanity),⁷⁴ the development of new technologies always presents

(stating the Russian armed forces' requirement to develop forces and resources for information confrontation); Memorandum from Sec'y of Def. on Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations (June 23, 2009), available at http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyber_command_gates_memo%5B1%5D.pdf (establishing a subordinate unified U.S. Cyber Command under U.S. Strategic Command for military cyberspace operations).

73. Streltsov, *supra* note 4, at 8; see also AUSTL. MINISTRY OF DEF., DEFENDING AUSTRALIA IN THE ASIA PACIFIC CENTURY: FORCE 2030, at 83 (2009), available at http://www.defence.gov.au/whitepaper/docs/defence_white_paper_2009.pdf ("The [Australian] Government has decided to invest in a major enhancement of Defence's cyber warfare capability."); REPUBLIC OF FR., THE FRENCH WHITE PAPER ON DEFENCE AND NATIONAL SECURITY 12 (2008), translated summary available at http://www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf (prescribing France's "establishment of an offensive cyber-war capability, part of which will come under the Joint Staff and the other part will be developed within specialised services"); U.K. CABINET OFFICE, CYBER SECURITY STRATEGY OF THE UNITED KINGDOM 14 (2009) [hereinafter UK CYBERSECURITY STRATEGY], available at <http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf> ("We recognise the need to develop military capabilities . . . to ensure we can defend against attack, and take steps against adversaries where necessary.").

74. See, e.g., Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Oct. 10, 1980, S. TREATY DOC. NO. 103-25 (1994), 1342 U.N.T.S. 137; Protocol I on Non-Detectable Fragments, Oct. 10, 1980, S. TREATY DOC. NO. 103-25 (1994), 1342 U.N.T.S. 168; Protocol II on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices, Oct. 10, 1980, S. TREATY DOC. NO. 105-1(A) (1997), 1342 U.N.T.S. 168; Protocol III on Prohibitions or Restrictions on the Use of Incendiary Weapons, Oct. 10, 1980, S. TREATY DOC. NO. 105-1(B) (1997), 1342 U.N.T.S. 171; Protocol IV on Blinding Laser Weapons, Oct. 13, 1995, S. TREATY DOC. NO. 105-1(C) (1997), 35 I.L.M. 1218; Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva Convention I]; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter Geneva Convention II]; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Geneva Convention IV]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 58, *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 3 [hereinafter Geneva Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 609 [hereinafter Geneva Protocol II]. As used herein, "Geneva Conventions" collectively refers to Geneva Convention I, Geneva Convention II, Geneva Convention III, Geneva Convention IV, Geneva Protocol I, and Geneva Protocol II.

difficulties for imposing limitations on the means and methods of warfare.⁷⁵ Sovereign nations not only negotiate such agreements cognizant of their own military strengths and weaknesses but also base their military doctrines and rules of engagement on their own interpretations of the relevant treaties and customary international law.⁷⁶ Without any controlling legal authorities for cyber conflicts today, there remains broad room for maneuver—both diplomatically and militarily.

Two of the key debates within the international community are (i) the extent to which the existing rules and norms of IHL are sufficiently applicable to cyber conflicts⁷⁷ and (ii) whether there is a need for *lex specialis* disarmament measures regarding information weapons.⁷⁸ Speaking on behalf of the European Union (EU) in 2001, Sweden made a submission to the U.N. Secretary-General:

EU is not of the view that, within the context of the General Assembly, the First Committee should be the main forum for discussing the issue of information security. Since the question mainly encompasses subjects other than disarmament and international security, EU believes there are other committees better suited for discussion of at least some of the aspects of the issue.⁷⁹

Then in 2004, both the United States and the United Kingdom officially specified that they opposed an international treaty limiting the military use of ICTs. Moreover, they each declared that current IHL provisions adequately “govern the use of such technologies.”⁸⁰

75. See CASSESE, *supra* note 13, at 402–03 (arguing that one of the major factors rendering the traditional international law of armed conflict “defective or inadequate in many respects” and thereby leading to the development of a new international body of law governing armed conflict was the development of “new agencies of destruction” such as the airplane and the atomic bomb (emphasis omitted)); Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT’L L. 391, 392 (2010) (“Military legal history has demonstrated that the law of war’s efficacy is a function of the law’s ability to keep pace with, as well as to address, how war is waged.”); cf. Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT’L L. 57, 88 (2010) (arguing that despite the number of governmental efforts utilized to encourage international cooperation in combating the “seemingly endless array” of cyber terrorist methods, “[n]one . . . is capable of completely securing the Internet”).

76. Cf. CASSESE, *supra* note 13, at 399 (highlighting the self-serving nature of nation-states and how that nature affects international law’s ability to constrain state actions).

77. See Watts, *supra* note 75, at 393 (remarking on the myriad legal issues—from “victims’ right to resort to force and the lawful use of preemptive or defensive [computer network attacks (CNAs)] (so-called *jus ad bellum* issues), to analyses of how the law regulating the conduct of hostilities (the *jus in bello*) applies to CNAs”—being debated regarding the adequacy of the law of war in the face of emerging uses of offensive CNAs).

78. See *id.* at 394 (“While assessments range from conclusions that existing law is largely adequate, to arguments to abandon the extant law entirely, to calls to draft a new *lex specialis*, broad consensus exists that CNAs producing destructive effects fully implicate law-of-war restraints and authorizations, both codified and customary.”).

79. *Developments in the Field* (July 3, 2001), *supra* note 51, at 5.

80. The relevant portion of the U.K. submission reads,

On the other hand, the parties to the SCO agreement, including Russia and China, have recognized a need to elaborate “collective measures regarding development of norms of international law to curb proliferation and use of information weapons that endangers the defensive capability, national and public security.”⁸¹ Although not a member of the SCO, Brazil forwarded a very similar position in its 2009 submission to the U.N. Secretary-General, asserting that “[t]he United Nations should also play a leading role in the discussions on the use of information and telecommunications as cyberwarfare in interstate conflict situations, paying special attention to the following aspects: . . . Establishment of a code of conduct for the use of information weapons.”⁸²

The net observation of state practice regarding the need for a *lex specialis* concerning the military use of ICTs is profound disagreement. Not only are there no generally accepted views at this time but the permanent members of the U.N. Security Council are themselves divided with the United States, United Kingdom, and France (presuming its concurrence with the 2001 EU submission) opposing new binding rules, while Russia and China would ostensibly favor them.⁸³ It is worth noting, however, that some of those official statements are several years old, and national policy positions may have changed. For example, President Obama’s speech on May 29, 2009, and the related White House Cyberspace Policy Review may have signaled a new willingness to discuss cyber conflicts as a matter of international security (and possibly arms control)—even though the United States is not yet prepared to negotiate any formally binding instruments.⁸⁴

What nations do of their own accord and how they respond to others’ actions will serve as precedents for future cyber conflicts. State practice creates a dual-track, recursive process by which sovereign governments individually or collectively interpret the rules of *jus ad bellum* and *jus in bello*; produce their own national strategies, declaratory policies, military doctrines, and rules of engagement; and then conduct activities that in turn influence

The United Kingdom does not, however, believe that there is a need for a multilateral instrument that would restrict the development or use of certain civil and/or military technologies. With respect to military applications of information technologies, such an instrument is unnecessary. The law of armed conflict, in particular the principles of necessity and proportionality, governs the use of such technologies.

Developments in the Field (June 23, 2004), *supra* note 51, at 11. The U.S. submission was equally clear in its determination: “With respect to military applications of information technology, an international convention is completely unnecessary. The law of armed conflict and its principles of necessity, proportionality, and limitation of collateral damage already govern the use of such technologies.” *Developments in the Field Add.* (Dec. 28, 2004), *supra* note 51, at 4.

81. SCO Agreement, *supra* note 17, art. 3.

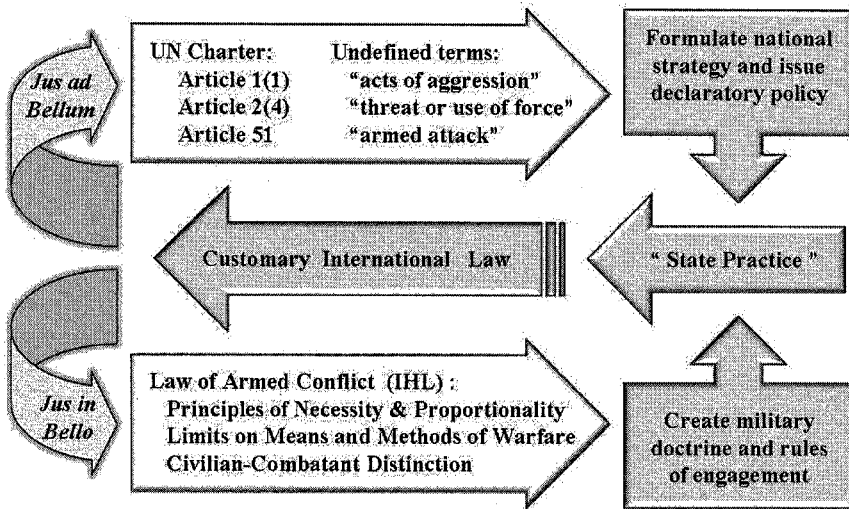
82. *Developments in the Field* (July 8, 2009), *supra* note 51, at 3–4.

83. See *supra* notes 78–82 and accompanying text.

84. See WHITE HOUSE, *supra* note 3 (providing a framework for engaging in international discussions about cybersecurity); Obama, *supra* note 70 (framing the problem of cybersecurity as an international problem).

customary international law and the future application of the U.N. Charter, Geneva Conventions, and other IHL provisions.

**Development Cycle of International Norms
for State Actors in Cyberspace**



IV. Strategic Considerations

A. State Responsibility

Besides playing an active role in the formation of customary international law through statecraft, sovereign nations also seek to pursue and protect their national interests while complying with accepted legal obligations. Having already examined the notion of sovereignty as it is being projected onto cyberspace and the importance of state practice, it is necessary to consider several substantive principles of public international law that have practical import when considering cyber conflicts. The inability to attribute deleterious events in a timely fashion was already acknowledged above, and one must now recognize that any sovereign efforts to regulate or monitor their national cyberspace not only require substantial resources but may also conflict with other public-policy interests, such as privacy and free speech. Even if sovereign control were desirable, publicly available technology has simply outpaced the ability of governments to perform fully effective law enforcement and national security procedures.⁸⁵

85. Interestingly, this is true of both developing nations whose state organs do not have the technical competence, requisite hardware and software, or judicial capacity to enforce laws as well as highly developed nations like the United States—whose legal culture currently precludes the level of systematic authentication and monitoring that would be necessary to completely quash

So, despite the pervasive will to exert sovereign authority over cyberspace, no state is currently able to completely deter, prevent, or even detect unwanted activity on or emanating from its ICT networks.⁸⁶ This limitation is a critical obstacle to applying the principle of state responsibility to the effects of state and nonstate actors alike. During the deliberations of the U.N. group of governmental experts in January 2010, for example, China proposed that sovereign states “have the responsibilities and rights to take necessary management measures to keep their domestic cyberspace and related infrastructure free from threats, disturbance, attack and sabotage.”⁸⁷ India was even more explicit in its discussion of that same topic:

By creating a networked society and being a part of [a] global networked economy, it is necessary for nation states to realise that they not only have a requirement to protect their own ICT infrastructure but at the same time have a responsibility to ensure that their ICT is not abused, either covertly or overtly, by others to target or attack the ICT infrastructure of another nation state.⁸⁸

Although this represents the same theory of imputed accountability for failure of a sovereign to mitigate nonstate actor threats to international peace and security that has been relied upon to impose liability in other circumstances—such as the refusal or inability of the de facto government of Afghanistan to prevent the Taliban and al Qaeda from planning and conducting terrorist operations from Afghan territory⁸⁹—it is unclear that any state is prepared (politically or technologically) to take full responsibility for all harm emanating from gateway routers, very small aperture terminals

cyber threats. See WHITE HOUSE, *supra* note 3 (stating that reform of U.S. legal structures is necessary to meet the changing needs of modern cybersecurity). In addition, many sovereign governments do not own or directly administer the critical information infrastructures in their countries—including the networks on which their own government and military entities rely. Finally, one cannot overlook the simple economic trade-off between the security and functionality of ICT networks. Thus far, no nation has made the necessary investment to develop a fully secure and functionally operative information infrastructure.

86. See generally ROSENZWEIG, *supra* note 34, at 14 (“The doctrine of ‘State responsibility’ has long been an established international law concept, but it has become particularly relevant in terms of assessing responsibility for cyber attacks.”).

87. China’s Contribution to the Report of the U.N. Group of Governmental Experts on Information Security 3 (January 2010) (on file with Texas Law Review).

88. India’s Contribution to the Report of the U.N. Group of Governmental Experts on Information Security 3 (January 2010) (on file with Texas Law Review). Russia alluded to the same principle when it asserted, “States and other subjects of international law should refrain of such actions against each other and should bear responsibility at international level for such actions in information space, carried out directly, under their jurisdiction or in the framework of international organizations of their membership.” Russia’s Contribution to the Report of the U.N. Group of Governmental Experts on Information Security 5 (January 2010) (on file with Texas Law Review).

89. See, e.g., Elisabeth Bumiller, *Bars Talks, Saying Hosts Will Share the Terrorists’ Fate*, N.Y. TIMES, Sept. 21, 2001, at A1 (“President Bush demanded tonight that Afghanistan’s leaders immediately deliver Osama bin Laden and his network and close down every terrorist camp in the country or face military attack by the United States.”).

(VSATs), wireless mobile devices, and other devices within its territory or jurisdiction.⁹⁰ Any sovereign's decision to support an international norm of state responsibility in cyberspace would need to be as much a practical consideration as one of legal principle.

According to two distinguished international-law scholars, Antonio Cassese and Ian Brownlie, the appropriate legal analysis for attributing responsibility for the actions of nonstate actors to host states themselves would necessarily rest upon the degree of due diligence or negligence exhibited by the sovereign.⁹¹ In other words, the state would not be held responsible for the act itself but would rather be held accountable for failing to fulfill a legal obligation that would have prevented the attendant harm. Outside the cyber context, the ILC has proposed that "[t]he State of origin shall take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof."⁹² In the absence of any international consensus on the norms for cyberspace, it would be very difficult to determine whether a state had performed adequate due diligence or taken the appropriate measures to avert harm in cyberspace.

B. *International Humanitarian Law*

The potential for cyber conflicts also poses several other legal and strategic difficulties concerning the notions of neutrality, perfidy, distinction, and humanity under existing IHL. While that list of topics is not exhaustive and none of them will be fully addressed or resolved here, they are all worth

90. This topic raises numerous legal and technical issues—including common-carrier provisions under U.S. telecommunications law and the requisite level of effective territorial control for legitimate sovereignty under public international law—that will not be addressed in any detail here due to space limitations.

91. Antonio Cassese states,

In the case of unlawful acts committed by *individuals not acting as de facto State officials*, for instance against foreigners or foreign authorities, the State on whose territory the acts were committed incurs international responsibility only if it did not act with due diligence: if it omitted to take the necessary measures to prevent attacks on foreigners or foreign assets, or, after perpetration of the unlawful acts, failed to search for and duly punish the authors of those acts, as well as pay compensation to the victims.

CASSESE, *supra* note 13, at 250. Ian Brownlie has similarly concluded,

There is general agreement among writers that the rule of non-responsibility cannot apply where the government concerned has failed to show due diligence. However, the decisions of tribunals and the other sources offer no definition of 'due diligence.' Obviously no very dogmatic definition would be appropriate, since what is involved is a standard which will vary according to the circumstances. And yet, if 'due diligence' be taken to denote a fairly high standard of conduct the exception would overwhelm the rule.

BROWNLIE, *supra* note 21, at 455.

92. Draft Articles on Prevention of Transboundary Harm from Hazardous Activities art. 1, in Report of the International Law Commission on the Work of Its Fifty-Third Session, U.N. GAOR, 56th Sess., Supp. No. 10, at 372, U.N. Doc. A/56/10 (Apr. 23, 2001–Aug. 10, 2001).

examining briefly because they collectively illustrate just how problematic certain aspects of cyber conflicts could be for the law.

If states cannot effectively monitor or control the data packets transiting their ICT networks or the electromagnetic waves permeating their airspace, then the traditional concept of neutrality may have to be revisited before it can be applied to cyber conflicts. Normally, belligerents are prohibited from using a neutral state's territory to deploy armaments or mount an armed attack.⁹³ Furthermore, a state can only maintain its neutrality by remaining impartial vis-à-vis opposing belligerents.⁹⁴ But, what if a neutral party did not know when its sovereignty was breached to conduct an attack or was technically incapable of restricting belligerents' use of its ICT networks without irreparably harming its own governmental functions or economy? What if the tools required to conduct or defend against a cyber attack needed to be pre-positioned in global networks to be most efficacious? What if a sovereign did not exercise due diligence in preventing its own subjects from criminally compromising foreign computer systems and later using them to attack a third sovereign nation?

The question of neutrality becomes even more complicated due to the uncertain legal status of cyberspace. If it is considered sovereign territory, then "[b]elligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power."⁹⁵ If, however, it is deemed a partial or complete commons, then perhaps "[t]he neutrality of a Power is not affected by the mere passage through its territorial waters of war-ships or prizes belonging to belligerents."⁹⁶ The analogy to information weapons (and the potential "prizes" of cyber conflict) transiting foreign ICT nodes is evident, but the appropriate legal norm is far from clear because the traditional notion of neutrality depends on both observable actions and the agreed legal status of the relevant medium where they take place.⁹⁷

Another long-standing principle of IHL is the prohibition on perfidy, which precludes "[a]cts inviting the confidence of an adversary to lead him

93. Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land arts. 1–4, Oct. 18, 1907, 36 Stat. 2310, 1 Bevans 654 [hereinafter Hague Convention V].

94. While "[a] neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals Every measure of restriction or prohibition taken by a neutral Power . . . must be impartially applied by it to both belligerents." *Id.* arts. 8–9.

95. *Id.* art. 2.

96. Convention Concerning the Rights and Duties of Neutral Powers in Naval War art. 10, Oct. 18, 1907, 36 Stat. 2415, 1 Bevans 723 [hereinafter Hague Convention XIII].

97. *See id.* art. 1 ("Belligerents are bound to respect the sovereign rights of neutral Powers and to abstain, in neutral territory or neutral waters, from any act which would, if knowingly permitted by any Power, constitute a violation of neutrality."). Not only is it unclear what would constitute a violation of neutrality in cyberspace, but it is equally questionable that a sovereign would even know when its rights had been violated in order to defend and preserve its neutrality.

to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence.”⁹⁸ Combatants are required to have distinctive signs or emblems and carry their arms openly;⁹⁹ accordingly, they are forbidden from feigning civilian, noncombatant status or using the insignia of enemy combatants during an attack.¹⁰⁰ The problematic nature of attribution in cyberspace, however, makes it nearly impossible to distinguish between the actions of lawful combatants (whether friend or adversary) and those of civilians. Without the equivalent of military emblems on information weapons, it becomes incredibly difficult to adhere to the principle of distinction and honor the prohibition against perfidy.¹⁰¹

From a strategic perspective, the IHL principles regarding perfidy, treachery, and chivalry are intended to ensure that certain humanitarian actions remain possible even during violent conflicts. Without them, quarter and succor would not be given, surrender would not be credible, and armistice would be meaningless. In a virtual realm where one could not identify the adversary, maintain the integrity of established symbols, or even trust the authenticity of directives allegedly issued by one’s own chain of command, uncertainty would reign and the human suffering of combatants and civilians alike could increase. Even those military strategists who compare cyber conflict to aerial warfare will know that IHL historically sought to apply these same principles to that medium.¹⁰²

The principles of distinction and discrimination also require that sovereigns take precautions to protect civilian entities from the dangers of war.¹⁰³ “[T]o the maximum extent feasible,” they are required to “remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives” as well as to “avoid locating military objectives within or near densely populated areas.”¹⁰⁴ Furthermore, they are prohibited from using civilians to “render certain points or areas immune from military operations.”¹⁰⁵ Those legal obligations to physically

98. Geneva Protocol I, *supra* note 74, art. 37(1).

99. Geneva Convention III, *supra* note 74, art. 4(A)(2); Geneva Protocol I, *supra* note 74, art. 44(3); Convention Respecting the Laws and Customs of War on Land, Annex of Regulations art. 1(2)–(3), Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631 [hereinafter Hague Convention IV Annex]. As used herein, “Hague Conventions” collectively refers to Hague Convention IV Annex, Hague Convention V, and Hague Convention XIII.

100. Geneva Protocol I, *supra* note 74, arts. 37(1), 39; Hague Convention IV Annex, *supra* note 99, art. 23(f).

101. For additional discussion of perfidy in cyberspace, see Streltsov, *supra* note 4, at 11–12.

102. See Draft Rules of Aerial Warfare arts. 3, 13, 15–16, in 17 AM. J. INT’L L. SUPP. 245, 246–48 (1923) (limiting the exercise of belligerent rights and the conduct of hostilities to military aircraft and personnel exhibiting distinctive emblems).

103. Geneva Protocol I, *supra* note 74, art. 58.

104. *Id.* art. 58(a)–(b).

105. Geneva Convention IV, *supra* note 74, art. 28; Geneva Protocol I, *supra* note 74, art. 51(7).

separate military and civilian objects become almost meaningless in the context of modern ICT networks. Today, the military often relies on the same communications nodes, navigation satellites, public utility grids, hardware and software, and technical personnel as the civilian populace.¹⁰⁶ Unless IHL is interpreted to require that government and military organizations build and utilize their own distinct information infrastructure—which is simply not feasible on either technical or economic grounds at this juncture—the collocation of key military targets with invaluable civilian assets is inevitable. In the end, military commanders will be left to judge what level of collateral damage is permissible under the principles of necessity and proportionality.

Another strategic consideration for cyber conflict under IHL is the extent to which the principle of humanity might actually require nation-states to use nonlethal information weapons in lieu of kinetic weapons if they would achieve the same military objective while producing fewer casualties (civilian or combatant) or shorter disruptions to the affected targets.¹⁰⁷ Perhaps temporarily disabling a radar system at an airport or rendering a power plant inoperable is more “humane” than permanently destroying those targets with ordnance, especially when civilian lives are dependent on them. The several examples offered in this section are certainly not the only difficulties for IHL in cyberspace, but they are illustrative of new technological concerns not previously envisioned by either the Hague Conventions or the Geneva Conventions.

C. Preventing Escalation

The strategic realities of geopolitics dictate that no command decisions regarding future cyber conflicts will be made in complete isolation and that governments will not be interpreting or applying the provisions of public international law in an abstract manner. Rather, their determinations will be driven by actual events and made out of necessity. Taken in that context, the unresolved *jus ad bellum* and *jus in bello* issues concerning cyberspace raise several major concerns. Most importantly, it will be the victim state—not the original “aggressor”—who will ultimately decide if specific actions constitute an “armed attack” or “use of force.” In other words, the victim state’s legal interpretations will govern for practical purposes as opposed to those of

106. See, e.g., WHITE HOUSE, *supra* note 3, at 17 (“The private sector, however, designs, builds, owns, and operates most of the network infrastructures that support government and private users alike.”); ROBERT H. ANDERSON & RICHARD O. HUNDLEY, RAND CORP., THE IMPLICATIONS OF COTS VULNERABILITIES FOR THE DOD AND CRITICAL U.S. INFRASTRUCTURES: WHAT CAN/SHOULD THE DOD DO? 1 (1998), <http://www.rand.org/pubs/papers/2009/P8031.pdf> (“Critical systems on which the security and safety of the United States depend are increasingly based on commercial off-the-shelf (COTS) software systems.”).

107. See, e.g., DAVID A. KOPLOW, DEATH BY MODERATION: THE U.S. MILITARY’S QUEST FOR USEABLE WEAPONS 232 (2010) (discussing how cyber weapons “may offer the most humane, barrier-free mechanisms imaginable for warfare”).

any foreign legal advisors who authorized such actions under their respective legal systems and military regulations. Moreover, information weapons have occasionally been compared to other weapons of mass destruction that threaten catastrophic consequences, suggesting the legal right to respond to cyber attacks—or imminent threats thereof—in any manner one sees fit.¹⁰⁸ Such a situation poses real concerns of escalation, where one state could view its own actions as permissible sanctions or reprisals but others would consider them impermissible acts of war.

Further compounding such tensions is the fact that current ICTs offer few solutions for mitigating such problems. Without positive attribution, there is no ability to monitor, verify, or signal in the traditional Cold War sense.¹⁰⁹ This in turn raises the question of whether or not cyber deterrence is even possible at this juncture.¹¹⁰ One final strategic consideration is the degree to which third parties, including nonstate actors, might be able to precipitate or escalate otherwise manageable conflicts between states. Once again, the improbability of real-time attribution poses a very significant obstacle to international peace and security in cyberspace, and that technical difficulty would only be exacerbated in cases where sovereigns employed nonstate actors—such as criminal or political groups—as proxies to commit cyber attacks on their behalf in order to avoid state responsibility.¹¹¹

Unfortunately, the same technological limitations, fears, and uncertainties that make tactical escalation a possibility would also complicate any strategic disarmament efforts. Clearly defined rules of state responsibility and demonstrable (or at least verifiable) national command-authority structures are two prerequisites for successful arms-control regimes. In the absence of either, international legal instruments proscribing the development, proliferation, or use of information weapons will be destined for failure.

108. See NATIONAL RESEARCH COUNCIL, *supra* note 2, at 296 (“U.S. declaratory policy regarding nuclear weapons suggests that the United States could respond to certain kinds of cyberattacks against it with nuclear weapons.”); David Talbot, *Russia’s Cyber Security Plans*, TECH. REV. EDITORS’ BLOG, April 16, 2010, <http://www.technologyreview.com/blog/editors/25050/> (quoting Russian Security Council member Vladislav Sherstuyuk’s statement that “there is much in common between nuclear and cyberweapons, because [cyberweapons] can affect a huge amount of people”).

109. See JAMES DENARDO, *THE AMATEUR STRATEGIST: INTUITIVE DETERRENCE THEORIES AND THE POLITICS OF THE NUCLEAR ARMS RACE* 48 (1995) (describing Cold War Era nuclear deterrence in terms of each nation reading the signals of other nations and striving to decrease uncertainty); THOMAS C. SCHELLING, *THE STRATEGY OF CONFLICT* 79–80 (1979) (recognizing the value of signals between parties in shaping a socially optimal outcome).

110. For a detailed discussion of the possibilities for deterrence in cyberspace, see Richard L. Kugler, *Deterrence of Cyber Attacks*, in *CYBERPOWER AND NATIONAL SECURITY* 309 (Franklin D. Kramer et al. eds., 2009).

111. See UK CYBERSECURITY STRATEGY, *supra* note 73, at 13 (“The use of proxies provides state actors with an extra level of deniability.”).

V. Conclusion

Today, the international community lacks consensus regarding the generally accepted principles of law applicable to cyber conflicts.¹¹² While all may agree that certain principles of IHL need to be respected, sovereign nations remain in vocal disagreement regarding the sufficiency of those provisions to regulate sovereign conduct in cyberspace. However, two things are certain. First, experience indicates that cyber threats will be propagated from those jurisdictions that criminals, terrorists, or other malicious actors find most favorable, i.e., those with the least stringent domestic regulations and the greatest inability to monitor or curtail malevolent Internet traffic. In legal terminology, that means the adversary will always have the “choice of venue,” which directly implies the second truism. Namely, the ultimate solution to the systemic insecurity that is engendered by a globally connected infrastructure will not be found in the reinterpretation or reform of any particular state’s legal authorities and enforcement capabilities. Similarly, unilateral declarations or actions are unlikely to resolve the common problems faced by all sovereigns. Cybersecurity has become a worldwide concern which requires the establishment of collective norms and cannot be adequately addressed by any nation in isolation.

Those sovereigns wishing to adequately protect their critical information infrastructures will also need to reconsider many of their competing domestic policy objectives. Only by marshaling all of their societal resources will they be able to truly safeguard the economic and political backbone of a modern nation. At least one historical analogy is haunting:

In most accounts, France in the late 1930s lacked a coherent national strategy to deal with the German threat. Such a strategy would have linked diplomatic schemes to military strategy, and industrial policy to military doctrine; in principle, it would have orchestrated every national strategic asset from labor power to health policy.¹¹³

Only through comprehensive national initiatives and the conclusion of a genuine international legal consensus will the devastating impacts of cyber conflicts that so many sovereigns now fear be averted, or at least mitigated.

112. See ESTONIAN CYBERSECURITY STRATEGY, *supra* note 34, at 17 (“So far, no binding international law on cyber security exists which expresses the common will of countries and which can serve as the basis for shaping national laws.”).

113. EUGENIA C. KIESLING, *ARMING AGAINST HITLER: FRANCE AND THE LIMITS OF MILITARY PLANNING* 6 (1996).

In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act: Judicial Recognition of Certain Warrantless Foreign Intelligence Surveillance*

Matthew A. Anzaldi** & Jonathan W. Gannon***

I. Introduction

Mere hours before adjourning for its August 2007 recess,¹ Congress amended the Foreign Intelligence Surveillance Act (FISA)² and enacted the Protect America Act of 2007.³ Congress took up the measure based upon concerns raised by the Director of National Intelligence (DNI) that FISA required immediate modernization in the face of a “heightened terrorist threat environment” to address the needs of the U.S. Intelligence Community and to remove FISA’s “requirement of a court order to collect foreign intelligence about foreign targets located overseas.”⁴ Among other things, the Protect America Act authorized the DNI and the Attorney General to conduct foreign intelligence surveillance concerning persons reasonably believed to be outside the United States without obtaining a warrant or other court order.⁵

Debate over the Protect America Act focused on the extent to which it safeguarded the privacy interests of U.S. persons.⁶ Supporters of the

* The views expressed in this Article are solely those of the authors and do not necessarily represent the views of any other person or entity, including the Department of Justice. This Article has been submitted for prepublication review pursuant to 28 C.F.R. § 17.18 (2009) and cleared for publication. The authors, among others, received the National Security Division Assistant Attorney General’s Award for Special Initiative for their work on the matter discussed in this Article. The authors would like to thank their colleagues at the Department of Justice and the other Symposium participants for their review and comments on this Article.

** Attorney Advisor, Office of Intelligence, National Security Division, U.S. Department of Justice. A.B., 1993, Duke University; J.D., 1996, Vanderbilt University Law School.

***Deputy Unit Chief, Office of Intelligence, National Security Division, U.S. Department of Justice. B.A., 1995, College of the Holy Cross; J.D., 2000, Vanderbilt University Law School.

1. See Eric Lichtblau et al., *Reported Drop in Surveillance Spurred a Law*, N.Y. TIMES, Aug. 11, 2007, at A1 (describing the “fever pitch” of negotiations going into the August recess).

2. Foreign Intelligence Surveillance Act of 1978, Pub L. No. 95-511, 92 Stat. 1783, (codified as amended in scattered titles of the U.S.C.).

3. Pub. L. No. 110-55, 121 Stat. 552 (to be codified at 50 U.S.C. §§ 1803, 1805a–1805c). For a discussion of the legislative history of the Protect America Act, see generally ELIZABETH B. BAZAN, CONG. RESEARCH SERV., P.L. 110-55, THE PROTECT AMERICA ACT OF 2007: MODIFICATIONS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2008), available at <http://www.fas.org/sgp/crs/intel/RL34143.pdf>.

4. S. REP. NO. 110-209, at 6 (2007).

5. Protect America Act § 2.

6. See FISA § 101 (codified at 50 U.S.C. § 1801(i) (2006)) (defining “United States person[s]” primarily as citizens and permanent resident aliens of the United States); S. REP. NO. 110-209, at 5

legislation argued that the Protect America Act would restore FISA's original balance between protections for persons communicating within the United States and the Executive Branch's traditional authority to conduct certain warrantless surveillance.⁷ Critics declared that the legislation would authorize unconstitutional, warrantless surveillance of the communications of U.S. persons, would transfer power from the courts to the Executive Branch, and would place excessive authority in the hands of the Attorney General and the DNI.⁸ About one thing, at least, supporters and critics agreed: the adjournment deadline did not afford the time necessary to analyze the legislation sufficiently.⁹ The legislation, therefore, included a six-month sunset provision.¹⁰ As one member noted, "To state the obvious: This is a very troublesome way to legislate."¹¹

During the following months, while Congress considered changes to the Protect America Act, a communications service provider challenged on Fourth Amendment grounds the constitutionality of the legislation in classified proceedings before the Foreign Intelligence Surveillance Court (FISC or FISA Court) and later, on appeal, before the Foreign Intelligence Surveillance Court of Review (Court of Review).¹² The Court of Review's

(describing how Director of National Intelligence J. Michael McConnell's proposal to modernize the Foreign Intelligence Surveillance Act intended to preserve "the privacy interests of persons in the United States").

7. See *Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 30 (2007) [hereinafter *Modernization of FISA*] (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice ("We can and should amend FISA to restore its original focus on foreign intelligence activities that substantially implicate the privacy interests of individuals in the United States.")).

8. See, e.g., American Civil Liberties Union, *ACLU Fact Sheet on the "Police America Act,"* (Aug. 7, 2007), <http://www.aclu.org/safefree/nsaspying/31203res20070807.html> (arguing that the Protect America Act "allows for massive, untargeted collection of international communications without court order or meaningful oversight by either Congress or the courts" and that the Act provides "no protections for the U.S. end of the phone call or email, leaving decisions about the collection, mining and use of Americans' private communications up to this administration").

9. For example, Senator Russ Feingold, who voted against the Protect America Act, called it a "cynical, cynical abuse of the process" when, in his view, the Bush Administration delayed negotiations on the bill and then rushed it through just before the August adjournment. David Sarasohn, *Rewriting the Surveillance Rules*, OREGONIAN, Oct. 10, 2007, at B8; see also Editorial, *Stampeding Congress, Again*, N.Y. TIMES, Aug. 3, 2007, at A18 (criticizing the Bush Administration for rushing the Act's passage just prior to the August recess). For statements by bill supporters alluding to the lack of time allowed for deliberation, see *infra* notes 11 and 93. But see 153 CONG. REC. S10,860 (daily ed. Aug. 3, 2007) (statement of Sen. Hatch) ("Is the excuse [for not passing the Act] that we might not have enough time before recess? Of course we have time. We'll make time.").

10. Protect America Act of 2007, Pub. L. No. 110-55, § 6, 121 Stat. 552, 557 (to be codified at 50 U.S.C. § 1803 n.3).

11. 153 CONG. REC. S10,869 (daily ed. Aug. 3, 2007) (statement of Sen. Specter). Senator Specter voted for the Protect America Act. *Id.* at S10,870; see also S. REP. NO. 110-209, at 6 ("The [Protect America Act] sparked serious concerns about its reach and scope [The Senate Select Committee on Intelligence] immediately began to review the Act's implementation.").

12. *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1007-08 (FISA Ct. Rev. 2008) [hereinafter *In re Directives*].

decision on this challenge in *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (In re Directives)*¹³ upheld the Protect America Act as implemented by the Executive Branch.¹⁴ In so doing, the Court of Review expressly recognized a foreign intelligence exception to the Warrant Clause of the Fourth Amendment “when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.”¹⁵ The Court of Review also held that the warrantless surveillance, as implemented, satisfied the Fourth Amendment’s reasonableness requirement, even when the government acquires communications of U.S. persons who are not the targets of the surveillance.¹⁶ These holdings answer some of the principal criticisms of the Protect America Act. They also are a contemporary reminder that certain surveillances and searches conducted by the Executive Branch without prior judicial review do not violate the Fourth Amendment, at least when such activity is expressly authorized by Congress and subject to appropriate privacy protections.

II. Executive Branch Authority to Collect Foreign Intelligence Without a Court Order Before Enactment of the Protect America Act

For much of the nation’s history, the Executive Branch exercised largely unchecked discretion in gathering foreign intelligence. That changed in 1978 with the enactment of FISA, but even then certain methods of foreign intelligence collection, including those later implicated in the Protect America Act, continued to involve only the Executive Branch.

A. Foreign Intelligence Collection Prior to 1978 and Resulting Abuses

Before FISA, the Executive Branch conducted surveillance for foreign intelligence purposes without significant oversight by Congress or the

13. *Id.* at 1004.

14. *Id.* at 1016. The decision discussed herein is only the second opinion released by the Court of Review, which is comprised of three judges from United States district courts or courts of appeals who have been publicly designated by the Chief Justice. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 103, 92 Stat. 1783, 1788 (codified at 50 U.S.C. § 1803(b) (2006)). Although the court entertained amicus briefs from the American Civil Liberties Union and the National Association of Criminal Defense Lawyers in *In re Sealed Case*, 310 F.3d 717, 719 (FISA Ct. Rev. 2002), that matter was an *ex parte* proceeding. *Id.* at 721 n.6.

15. *In re Directives*, 551 F.3d at 1012. The Fourth Amendment provides,

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the places to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

16. *In re Directives*, 551 F.3d at 1015.

courts.¹⁷ Beginning with George Washington, a “master of military espionage,”¹⁸ presidents had conducted surveillance to collect foreign intelligence using an evolving array of techniques to account for changing technologies.¹⁹ Electronic surveillance—the interception of communications as they travel on a wire—began shortly after the development of electronic communication.²⁰ Electronic surveillance of wartime communications was conducted as far back as the Civil War, and President Wilson ordered the censorship of messages sent via wire during World War I.²¹ Before the country’s entry into World War II, President Roosevelt also authorized the warrantless surveillance of “persons suspected of subversive activities against the Government of the United States, including suspected spies.”²²

At the time, electronic surveillance implemented solely by the Executive Branch did not raise Fourth Amendment concerns because, as held by the Supreme Court in *Olmstead v. United States*,²³ wiretapping was not considered a search within the meaning of the Fourth Amendment.²⁴ The Supreme Court changed course in 1967, holding in *Katz v. United States*²⁵ that electronic surveillance implicated the Fourth Amendment.²⁶ Still, even after *Katz* recognized Fourth Amendment protections for certain electronic

17. See DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 3-2 (2007) (describing how, before FISA’s 1978 enactment, electronic surveillance was subject to little or no congressional or legislative oversight). The President derives the power to gather intelligence from his Article II authorities. Specifically, the President is Commander in Chief of the Armed Forces and controls the foreign affairs of the United States. U.S. CONST. art. II, § 2. The Supreme Court has recognized that the President “is the sole organ of the nation in its external relations, and its sole representative with foreign nations.” *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936) (citation omitted). Extending from these responsibilities is the President’s constitutional responsibility to protect the nation from foreign threats. U.S. DEP’T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 7 (2006) [hereinafter DOJ WHITEPAPER] (“[T]he Founders . . . intended that the President would have the primary responsibility and necessary authority as Commander in Chief and Chief Executive to protect the Nation and to conduct the Nation’s foreign affairs.”).

18. RHODRI JEFFREYS-JONES, CLOAK AND DOLLAR: A HISTORY OF AMERICAN SECRET INTELLIGENCE 11 (2d ed. 2003); see also ALLEN W. DULLES, THE CRAFT OF INTELLIGENCE 49 (1st ed. 1965) (discussing Washington’s observation in 1777 that “[t]he necessity of procuring good intelligence is apparent and need not be further urged”).

19. See, e.g., DOJ WHITEPAPER, *supra* note 17, at 14–16 (2006) (describing certain aspects of the history of wartime surveillance).

20. KRIS & WILSON, *supra* note 17, at 3-3 (citation omitted).

21. DOJ WHITEPAPER, *supra* note 17, at 16 (citing G.J.A. O’TOOLE, THE ENCYCLOPEDIA OF AMERICAN INTELLIGENCE AND ESPIONAGE 498 (1988) and Exec. Order No. 2604 (Apr. 28, 1917)).

22. KRIS & WILSON, *supra* note 17, at 3-6.

23. 277 U.S. 438 (1928).

24. *Id.* at 465 (“The language of the [Fourth] Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant’s house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.”).

25. 389 U.S. 347 (1967).

26. *Id.* at 353–54.

communications, the Executive Branch continued to operate without judicial or legislative checks.²⁷

Congress subsequently sought to regulate government wiretapping, but only in the context of criminal investigations.²⁸ In response to the Supreme Court's decisions in *Katz* and *Berger v. New York*,²⁹ and in an era of "increasing use and sophistication of electronic surveillance,"³⁰ Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III).³¹ While Title III barred electronic surveillance except under the circumstances set forth in the statute, Congress expressly avoided the regulation of foreign intelligence surveillance.³²

The Supreme Court also generally remained silent on the question of Fourth Amendment protections and foreign intelligence gathering. In *Katz*, the Court stated that its holding did not apply to a situation involving national security: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."³³ Several years later in *United States v. United States District Court (Keith)*,³⁴ the Government argued that § 2511(3) of Title III authorized warrantless surveillance of a domestic radical group.³⁵ The Court steered clear of the question of

27. DOJ WHITEPAPER, *supra* note 17, at 8, 17.

28. Congress enacted a criminal penalty prohibiting wiretapping of telephones during World War I and made it a crime for any person without the consent of the sender to "intercept and divulge or publish the contents of wire and radio communications" in § 605 of the Federal Communications Act of 1934. 47 U.S.C. § 605 (1934); KRIS & WILSON, *supra* note 17, at 3-3 to 3-5.

29. 388 U.S. 41, 44 (1967) (holding a New York statute regulating electronic eavesdropping to be unconstitutional).

30. KRIS & WILSON, *supra* note 17, at 3-13.

31. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801-804, 82 Stat. 197 (1968) (codified at 18 U.S.C. §§ 2510-2522 (2006)).

32. See JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE 9-5 (2007) ("Because a court order authorizing FISA surveillance differs in significant ways from a conventional search warrant, however, the adoption of FISA did not itself resolve other questions about when and under what conditions the Constitution permits foreign intelligence surveillance."). As enacted in 1968, 18 U.S.C. § 2511(3) provided, among other things, that nothing in Title III or § 605 of the Federal Communications Act of 1934 "shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, [or] to obtain foreign intelligence information deemed essential to the security of the United States." 18 U.S.C. § 2511(3) (1970). This provision was removed in 1978. CARR & BELLIA, *supra*, at 9-4; see also *id.* at 9-2 ("Section 2511(3) was intended as a codification of the legislative 'hands off' attitude which had prevailed under Title III's predecessor." (citations omitted)).

33. *Katz v. United States*, 389 U.S. 347, 358 n.23 (1967). Seizing upon the majority's caveat for national security, Justice White observed that "[w]e should not require the warrant procedure . . . if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable." *Id.* at 364 (White, J., concurring).

34. 407 U.S. 297 (1972)

35. *Id.* at 303.

warrantless surveillance for foreign intelligence gathering.³⁶ In concluding that the warrant requirement applied to investigations of domestic security threats, the *Keith* Court expressly reserved the question of whether the Warrant Clause applied to foreign intelligence surveillance and discussed several sources supporting the “view that warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved.”³⁷

This era of Executive Branch flexibility and warrantless foreign intelligence wiretapping came to an end with the well-documented abuses of the civil rights of U.S. persons uncovered by Congress through the Church Committee.³⁸ While the Intelligence Community often began investigations with legitimate national security concerns, the investigations “descended a slippery slope, beginning with efforts to counter foreign threats to national security and evolving to gather information about peaceful domestic groups lobbying for political change, such as equal rights for racial minorities and women.”³⁹ The abuses “included routine opening and reading of vast amounts of first-class mail and telegrams.”⁴⁰ One program run by the National Security Agency (NSA) was called “Operation Shamrock.”⁴¹ Originally intended to “obtain the enciphered telegrams of certain foreign targets,” Operation Shamrock expanded significantly over time to become at that time “the largest government interception program affecting Americans.”⁴² As a result of the program, from approximately 1945 to 1975 the NSA received copies of millions of international telegrams sent to, from,

36. *See id.* at 321–22 (“[T]his case involves only the domestic aspects of national security. We . . . express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents.”). Perhaps foreshadowing the creation of the FISC, the *Keith* Court rejected the Government’s argument that “internal security matters are too subtle and complex for judicial evaluation There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases.” *Id.* at 320. The Supreme Court further suggested that Congress should consider protective standards for domestic security cases different than those for criminal cases (Title III), including applications to a “specially designated court.” *Id.* at 323.

37. *Id.* at 322 n.20. As will be described below, while the Supreme Court has remained silent on the specific issue, prior to the decision discussed herein courts of appeals in the pre- and post-FISA context have held that the President has authority to conduct warrantless surveillance in cases involving foreign intelligence collection. *See infra* text accompanying notes 135–39.

38. In January 1975, the Senate created the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, chaired by Senator Frank Church, to investigate the activities of intelligence agencies. L. Britt Snider, *Congressional Oversight of Intelligence: Some Reflections on the Last 25 Years*, at 1 n.3, <http://www.law.duke.edu/lens/downloads/snider.pdf>. In February 1975, the House of Representatives established the Select Committee on Intelligence, chaired by Representative Otis Pike, for the same purpose. *Id.*

39. KRIS & WILSON, *supra* note 17, at 2–3.

40. *Id.*

41. S. REP. NO. 94-755, at 740 (1976).

42. *Id.*

or transiting the United States; in later years, the NSA reviewed approximately 150,000 telegrams per month.⁴³

B. 1978 to 2007: Executive Branch Adjustment to FISA

With the enactment of FISA in 1978, Congress entered the field of electronic surveillance for foreign intelligence purposes.⁴⁴ Congress enacted FISA to establish “a statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes.”⁴⁵ When FISA applies, it generally requires the government to seek an order from the FISC approving the use of “electronic surveillance” to obtain “foreign intelligence information,” which is defined as, *inter alia*, information that relates to the ability of the United States to protect against espionage, international terrorism, and other acts committed by foreign powers or their agents, as well as other information pertaining to the national defense and foreign affairs of the United States.⁴⁶ Among other things, the FISC must find that the government has established probable cause to believe that (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power, and (2) the target is using or is about to use the facility at which surveillance will be directed.⁴⁷ The FISC must also find that the minimization procedures proposed by the government are “reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting U.S. persons consistent with

43. *Id.*

44. Oversight of the intelligence agencies previously had fallen largely to subcommittees of the Senate and House Armed Services Committees. See Snider, *supra* note 38, at 2 (“Such oversight, as there was, was carried out in secret and in a relative vacuum.”). Congress later established committees specifically designed to conduct oversight of intelligence activities: the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). The Senate created SSCI in 1976 as the successor to the Church Committee, and the House created HPSCI in 1977 as the successor to the Pike Committee. See L. BRITT SNIDER, *THE AGENCY AND THE HILL: CIA’S RELATIONSHIP WITH CONGRESS, 1946–2004*, at 51, 53 (2008) (describing the inception of those committees). The Protect America Act contained certain reporting requirements to Congress, such as section four, beyond those in FISA generally. See, e.g., 50 U.S.C. § 1808 (2006) (requiring the Attorney General to report semi-annually to the SSCI and HPSCI on the government’s electronic surveillance activities).

45. H.R. REP. NO. 95-1283, at 22 (1978), reprinted in 1978 U.S.C.C.A.N. 3904, 3923–24.

46. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783, 1784 (codified at 50 U.S.C. § 1801(e) (2006)). The legislative history indicates that Congress specifically excluded from FISA certain Executive Branch authorities, including “international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance . . . conducted outside the United States.” S. REP. NO. 95-604, at 64 (1978); see also H.R. REP. NO. 95-1283, at 27 (1978), reprinted in 1978 U.S.C.C.A.N. 3904, 3928–29 (“The Committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillance.”).

47. FISA § 101. As noted below, the Protect America Act specifically provided that the government need not provide an individual probable cause statement for each target or facility. See *infra* note 102 and accompanying text.

the need of the United States to obtain, produce, and disseminate foreign intelligence information.”⁴⁸

FISA’s definition of electronic surveillance determines the reach of the statute, and by adopting the definition, Congress left untouched much of the foreign intelligence collection that was directed overseas and conducted solely on the basis of Executive Branch authority.⁴⁹ Only electronic surveillance, as defined in four parts, requires judicial approval.⁵⁰ The first definition of electronic surveillance is the acquisition of a “wire or radio communication” to or from “a particular, known United States person who is in the United States”⁵¹ This definition does not regulate the surveillance of targets located outside the United States.⁵² The second definition of electronic surveillance is the acquisition of a “wire communication,” defined as a communication carried on a wire by common carriers, to or from someone in the United States.⁵³ This definition did not regulate the surveillance of the most common manner of international communications.⁵⁴ At the time of

48. FISA § 101. Section 1801(h) defines “minimization procedures” in four parts, the most pertinent of which is quoted above. As discussed below, the Protect America Act incorporated FISA’s general definition of minimization procedures. *See infra* note 101 and accompanying text.

49. As noted at the SSCI hearing in May 2007, FISA “does not apply where all parties to a communication are located abroad. Purely foreign communications are simply beyond FISA’s ambit.” *Modernization of FISA, supra* note 7, at 130 (statement of David S. Kris).

50. FISA itself recognizes several instances when the Executive Branch could conduct warrantless “electronic surveillance.” First, 50 U.S.C. § 1802 permits surveillance without judicial approval for periods of up to one year based solely upon a certification of the Attorney General when either the surveillance is solely directed at the acquisition of (1) the “contents of communications transmitted by means of communications used exclusively between or among foreign powers,” or (2) “technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power.” FISA § 102. Moreover, the government may conduct electronic surveillance upon oral authorization of the Attorney General in emergency situations. *Id.* § 105. The period of surveillance for an emergency authorization without a warrant has been extended from 24 hours (1978) to 72 hours (2001) to seven days in the FISA Amendments Act of 2008. Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2439–40 (to be codified at 50 U.S.C. § 1881(a)). An application must be submitted to the FISC after such authorization. FISA § 105. Third, the Executive Branch may conduct electronic surveillance without a warrant for fifteen calendar days after a congressional declaration of war. *Id.* § 111. Finally, FISA permits certain testing of electronic equipment and training of intelligence personnel without judicial approval. *Id.* § 105.

51. FISA § 101. During the Protect America Act debate, Administration officials sought to reassure Congress that FISA’s reach had not changed with respect to this definition of electronic surveillance. *See, e.g., Modernization of FISA, supra* note 7, at 27 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice) (“[I]f the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence purposes, it is within FISA’s scope, period.”); *id.* at 12 (statement of J. Michael McConnell, Director of National Intelligence) (“Another thing that this proposed legislation does *not* do is change the law or procedures governing how NSA, or any other government agency, treats information concerning United States persons.”).

52. FISA § 101.

53. *Id.*

54. *See id.* (excluding satellite transmissions from this definition of electronic surveillance).

FISA's enactment, most international communications were carried primarily by satellite (i.e., radio), not wire.⁵⁵

The third definition of electronic surveillance applies to the acquisition of a "radio communication" only when "both the sender and all intended recipients are located within the United States."⁵⁶ Here, too, the definition does not regulate the surveillance of targets outside the United States.⁵⁷ Finally, the fourth definition of electronic surveillance relates to the "installation of an electronic, mechanical, or other surveillance device in the United States" but excludes information acquired from a "wire or radio communication."⁵⁸ As with the second definition, this definition of electronic surveillance excluded, as a matter of communication technology, the most common form of international communications: satellite.⁵⁹

These definitions made FISA's scope, particularly with respect to the international communications of targets outside the United States, to some extent dependent on the communication technology in use at a given time.⁶⁰

55. *Modernization of FISA*, *supra* note 7, at 28–29 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice); *cf.* David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: A Working Paper of the Series on Counterterrorism and American Statutory Law* 7–13 (Brookings Inst., Geo. Univ. Law Center, & Hoover Inst., Paper No. 1, 2007), available at http://www.brookings.edu/~media/Files/rc/papers/2007/1115_nationalsecurity_kris/1115_nationalsecurity_kris.pdf (estimating that between one-half and two-thirds of overseas calls were carried on satellites at the time of FISA's enactment).

56. FISA § 101.

57. *Id.*

58. *Id.*; see also H.R. REP. NO. 95-1283, at 52 (1978), reprinted in 1978 U.S.C.C.A.N. 3904, 3953–54 (noting that § 1801(f)(4) was "not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States").

59. FISA § 101.

60. The Executive Branch developed procedures for the conduct of foreign intelligence, including foreign intelligence gathering outside of FISA. The enactment of FISA in 1978 created the framework within which the Executive Branch conducted electronic surveillance within the United States for foreign intelligence purposes, and applications to the FISC increased during subsequent years. Executive Order 12,333, which has been amended as recently as 2008, outlines the responsibilities and limitations of the agencies of the Intelligence Community. Exec. Order No. 13,462, 73 Fed. Reg. 11,805 (Feb. 29, 2008). For example, the Attorney General maintained certain authority to authorize warrantless surveillance through section 2.5 of Executive Order 12,333, which among other things regulates the use of any technique against a U.S. person outside the United States. See Exec. Order No. 12,333, 3 C.F.R. 200 (1982), as amended by Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008), reprinted as amended in 50 U.S.C. § 401 (2006) (empowering the Attorney General to use techniques "for which a warrant would be required" against U.S. persons abroad who are thought to be an "agent of a foreign power"). Section 2.5 provides in relevant part:

The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that . . . the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.

If such international communications were carried by radio and satellite, FISA did not require a court order for government surveillance; if they were carried by wire, FISA might require an order.

III. The Protect America Act

A. *Debating the Protect America Act*

Before passage of the Protect America Act, changes in communications technology had, according to Administration officials, increased FISA's scope at the expense of Executive Branch authority.⁶¹ International communications, once mostly transmitted by satellite, were now transmitted by wire.⁶² New methods of communicating, including e-mail, became commonplace.⁶³ In summary, by operation of FISA's definition of electronic surveillance, FISA grew to encompass the surveillance of foreign intelligence targets outside the United States where, in the past, that surveillance might have been conducted without the requirement of a FISC order.⁶⁴

Changes in communications technology alone did not lead to serious proposals to restore FISA's original scope. Rather, plans to update FISA followed a new threat to national security and the increased (and, some claimed, consuming) number of applications for FISC authorization to target persons outside the United States.⁶⁵ These plans got a push after "any elec-

Id. As noted below, FISA now requires that such surveillance receive FISC approval. *See infra* text accompanying notes 232–33. Agencies have implemented the Executive Order through specific regulations. For example, Department of Defense (DOD) regulations require a statement of facts demonstrating probable cause and necessity and a statement of the period during which the surveillance was thought to be required, not to exceed 90 days. Department of Defense, DOD 5240.1-R, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons, 25–27 (Dec. 1982). This durational limit is the same as the limit authorized for an electronic surveillance order of a U.S. person pursuant to 50 U.S.C. § 1805. FISA § 105(d)(1). As discussed below, these procedures played an important role in the Court of Review's holding that the government acted reasonably under the Fourth Amendment in implementing the Protect America Act. *See In re Directives*, 551 F.3d 1004, 1013–14 (FISA Ct. Rev. 2008) (asserting that the procedures "serve to allay the probable cause concern"); *infra* subpart IV(B).

61. *Modernization of FISA*, *supra* note 7, at 29–30 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice). NSA had earlier raised issues concerning tension between FISA's scope and NSA's collections given technological advances. *See* Memorandum from Mary C. Lawton, Counsel for Intelligence Policy, U.S. Dep't of Justice, to Dan Levin, Office of the Deputy Attorney Gen., U.S. Dep't of Justice 1 (Nov. 1, 1990), available at http://gulcfac.typepad.com/georgetown_university_law/files/Lawton.1990.FISA.Memo.clean.pdf (noting that the Department of Justice had been working with NSA for the previous three years to develop amendments to FISA "to meet a need created by technological advances").

62. *Modernization of FISA*, *supra* note 7, at 30 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice).

63. *Id.* at 6 (statement of J. Michael McConnell, Director of National Intelligence).

64. *Id.* at 6–7 (statement of J. Michael McConnell, Director of National Intelligence).

65. As noted by Administration officials during the Protect America Act debate, the preeminent threat to the United States at the time of FISA's enactment was espionage by the Soviet Union and its agents and terrorism threats stemming from groups such as Black September, the Baader-Meinhof Group, and the Japanese Red Army, not international terrorism from groups such as al

tronic surveillance that was occurring as a part of the Terrorist Surveillance Program” (TSP) moved from Executive Branch authorization to FISC authorization in January 2007.⁶⁶

In the aftermath of the September 11, 2001 terrorist attacks, the use of FISA expanded dramatically.⁶⁷ The Director of the NSA stated in 2007 that FISA was “the key to the war on terrorism.”⁶⁸ Shortly after September 11, 2001, however, President George W. Bush authorized the NSA to operate outside of FISA “to intercept communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations.”⁶⁹ This authorization and the government’s subsequent effort to bring these activities before the FISC contributed in part to the legislative debate surrounding the Protect America Act. Specifically, on January 10, 2007, the FISC issued orders authorizing the government “to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization.”⁷⁰ Later in 2007, in response to a request to renew the January 2007 FISA orders, a different FISC judge issued a subsequent ruling in May 2007 that the DNI and others apparently could not accept.⁷¹ The Executive Branch turned to Congress to act.⁷²

Qaeda. *Modernization of FISA*, *supra* note 7, at 28 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice).

66. See U.S. DEP’T OF JUSTICE, NATIONAL SECURITY DIVISION PROGRESS REPORT 2 (2008) [hereinafter NSD PROGRESS REPORT] (detailing the National Security Division’s role in legislation to update FISA); Letter from Alberto Gonzales, Att’y Gen., to Patrick Leahy, Chairman, Senate Comm. on the Judiciary and Arlen Specter, Ranking Minority Member, Senate Comm. on the Judiciary 1 (Jan. 17, 2007), available at www.fas.org/irp/agency/doj/fisa/ag011707.pdf [hereinafter January 2007 Attorney General Letter]; see also James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1 (describing an NSA collection).

67. As required by FISA, the Department of Justice reports semi-annually to Congress the number of applications filed with the FISC. See Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 108, 93 Stat. 1783, 1783 (codified at 50 U.S.C. § 1808(a)) (requiring the Attorney General to report on FISA surveillance to the SSCI and HPSCI). The number of FISA applications increased from 932 in 2001 to 2371 in 2007. See KRIS & WILSON, *supra* note 17, app. G, at G-3 to G-35 (collecting annual reports for calendar years 1980 to 2006); Report from Principal Dep. Att’y Gen. Brian A. Benzckowski to Sen. Harry Reid (Apr. 30, 2008), available at http://www.justice.gov/nsd/foia/reading_room/2007fisa-ltr.pdf (containing 2007 annual report to Congress). The number of applications dropped to 2082 in 2008, the year after the Protect America Act’s enactment. Report from Ass’t Att’y Gen. Ronald Weich to Sen. Harry Reid (May 14, 2009), available at http://www.justice.gov/nsd/foia/reading_room/2008fisa-ltr.pdf.

68. *Modernization of FISA*, *supra* note 7, at 48 (testimony by Keith B. Alexander, Director, National Security Agency).

69. DOJ WHITEPAPER, *supra* note 17, at 1. A discussion of the NSA’s surveillance activities other than their effect on the legislative debate is outside the scope of this Article.

70. January 2007 Attorney General Letter, *supra* note 66, at 1.

71. S. REP. NO. 110-209, at 5 (2007). The report describes the situation as follows:

At the end of May 2007, however, attention was drawn to a ruling of the FISA Court. When a second judge of the FISA Court considered renewal of the January 2007 FISA orders, he issued a ruling that the DNI later described as significantly diverting NSA analysts from their counterterrorism mission to provide information to the Court.

In response to a request from the Senate Select Committee on Intelligence (SSCI), on April 12, 2007, the DNI submitted a proposal to Congress to modernize FISA.⁷³ While recognizing that FISA “provides the legal framework through which the Intelligence Community lawfully collects information about those who pose national security threats to our country,” the Department of Justice and Office of the DNI stated that the proposed legislation’s “core objective was to bring FISA up to date with the revolution in telecommunications technology that has taken place since 1978, while continuing to protect the privacy interests of persons located in the United States.”⁷⁴

On May 1, 2007, SSCI held the only significant hearing on FISA modernization before the Protect America Act’s enactment.⁷⁵ The hearing foreshadowed the arguments for and against the initiative that would arise during the debate a few months later.⁷⁶ The DNI, the Director of the NSA

Id.

72. Similar to the events leading to the original passage of FISA, the Protect America Act debate also occurred against the backdrop of recently revealed abuses in the Intelligence Community. In March 2007, the Department of Justice’s Inspector General released a highly critical report of the FBI’s use of national security letters from 2003 to 2005. U.S. DEP’T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF NATIONAL SECURITY LETTERS (2007), <http://www.justice.gov/oig/special/s0703b/final.pdf>. Critics of the FISA modernization efforts seized upon the misuse of the letters in advocating against increased Executive Branch authority. See, e.g., *Modernization of FISA*, *supra* note 7, at 111 (statement of Caroline Frederickson, American Civil Liberties Union) (“In light of recent revelations that the government is gravely abusing the authorities it already has, allowing this exponential increase in spying authority would not only be unconstitutional, but irresponsible.”).

73. S. REP. NO. 110-209, at 2; see also Foreign Intelligence Surveillance Modernization Act of 2007, H.R. 3782, 110th Cong. (1st Sess. 2007), available at <http://www.fas.org/irp/news/2007/04/fisa-proposal.pdf>. While the government’s submission in April 2007 included numerous proposed revisions, including liability protection provisions for service providers, this Article focuses on the proposed revision to the definition of electronic surveillance.

74. Press Release, U.S. Dep’t of Justice, Fact Sheet: Title IV of the Fiscal Year 2008 Intelligence Authorization Act, Matters Related to the Foreign Intelligence Surveillance Act (Apr. 13, 2007), http://www.justice.gov/opa/pr/2007/April/07_nsd_247.html.

75. See S. REP. NO. 111-6, at 2–3 (2008) (reviewing the background of the FISA Amendments Act of 2008 and the Protect America Act of 2007 and indicating that “[o]n May 1, 2007, the Committee [SSCI] held a public hearing to enable the Administration to explain as openly as possible why the legislation it was proposing should be enacted” and that it also held classified hearings); see also *Modernization of FISA*, *supra* note 7, at 1 (statement of Sen. John D. Rockefeller, Chairman, S. Select Comm. on Intelligence) (“The Select Committee on Intelligence meets today in open session, something we don’t often do, to consider whether the scope and application regarding the Surveillance Act needs to change to reflect the evolving needs . . . of foreign intelligence.”).

76. Compare, *Modernization of FISA*, *supra* note 7, at 54–55 (testimony by J. Michael McConnell, Director of National Intelligence & Keith B. Alexander, Director, National Security Agency) (questioning whether the proposed modernizations of FISA would allow intelligence agencies to investigate U.S. persons without obtaining a warrant), with 153 CONG. REC. S10,861 (daily ed. Aug. 3, 2007) (statement of Sen. Feingold) (denouncing the proposed legislation as authorizing “warrantless searches of Americans’ phone calls, e-mails, homes, offices, and personal records”).

(DIRNSA), and the Assistant Attorney General for National Security (AAG) testified in person at the hearing, and experts on national security and civil liberties submitted statements to the Committee.⁷⁷

The DNI argued that the Administration's proposal sought to make FISA "technology neutral" by carving foreign-to-foreign communications of non-U.S. persons out of FISA's definition of electronic surveillance.⁷⁸ At the hearing, the DNI emphasized FISA's preeminent role in this area, noting that when he left the NSA in 1996 FISA's role was "not significant . . . And today it is probably *the* most significant ability we have to target and be successful in preventing attacks."⁷⁹ Administration officials also seized upon the legislative history as demonstrating Congress's reluctance to encroach upon Executive Branch authority.⁸⁰

Critics of the proposal dismissed the effort to update FISA, warning that under the "guise of 'tech neutrality'" the legislation would authorize warrantless surveillance of "virtually all communications in any form by Americans with anyone, including other Americans, located overseas."⁸¹

77. S. REP. NO. 110-209, at 5. For a complete list of the statements for the records at the May 2007 SSCI hearing and the government's proposal, see *Modernization of FISA*, *supra* note 7, at III. This Article generally focuses on the testimony and debate leading up to the enactment of the Protect America Act.

78. *Modernization of FISA*, *supra* note 7, at 18 (testimony by J. Michael McConnell, Director of National Intelligence) ("In today's threat environment, the FISA legislation is not agile enough to handle the country's intelligence needs."). The AAG also focused on FISA's definition of electronic surveillance, arguing that "unanticipated advances in technology [since 1978] have wreaked havoc on the delicate balance that Congress originally struck [in FISA]." *Id.* at 29–30 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice). Thus, the government's proposed modification sought to shift the focus from "*how* a communication travels or *where* it is intercepted . . . to *who is the subject of the surveillance.*" *Id.* at 30.

79. *Modernization of FISA*, *supra* note 7, at 48 (testimony by J. Michael McConnell, Director of National Intelligence). The DNI also noted that under the existing statute the Intelligence Community was "often required to make a showing of probable cause, a notion derived from the Fourth Amendment, in order to target for surveillance the communications of a foreign person overseas. Frequently, although not always, that person's communications are with another foreign person overseas." *Id.* at 11–12 (statement of J. Michael McConnell, Director of National Intelligence); *cf. id.* at 19 ("[T]here were gaps in NSA's coverage of foreign communications and in FBI's coverage of domestic communications." (quoting S. REP. NO. 107-351, at 36 (2002))).

80. For example, Assistant Attorney General Kenneth L. Wainstein has testified that:
Congress recognized the importance of striking an appropriate balance between the need to protect the civil liberties of Americans, and the imperative that the Government be able to collect effectively foreign intelligence information that is vital to the national security. . . . [Congress] also recognized that the terrain in which it was legislating touched upon a core Executive Branch function—the Executive's constitutional responsibility to protect the United States from foreign threats.

Modernization of FISA, *supra* note 7, at 25 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. for National Security, United States Department of Justice).

81. *Modernization of FISA*, *supra* note 7, at 187 (statement of Kate Martin, Director, Lisa Graves, Deputy Director, Center for National Security Studies); *see also id.* at 107 (statement of Caroline Frederickson, American Civil Liberties Union) ("Technology may have changed, but the

Another critic dismissed the need to rush to amend FISA, noting that FISA had been amended six times since September 11, 2001.⁸² Despite these and other criticisms, including a general concern that the proposal was “a grasp for spying authority worthy of Big Brother and George Orwell’s *1984*,”⁸³ several supporters and critics of amending FISA alike noted that communications between non-U.S. persons outside the United States are not subject to FISA.⁸⁴

Beginning in late July 2007, the House of Representatives and the Senate considered several bills designed to meet the requirements of the DNI.⁸⁵ Critics expressed concern that the Protect America Act authorized “warrantless searches of Americans’ phone calls,⁸⁶ e-mails, homes, offices

Fourth Amendment has not. Except for a very few circumstances, warrants are required to listen to phone calls or otherwise access the content of a communication . . .”).

82. See *Modernization of FISA*, *supra* note 7, at 99 (statement of Bruce Fein) (“The government has not come close to demonstrating a national security need that would justify the alarming encroachments on the right to be left alone—the liberty most cherished in civilized nations—that would be effectuated by the proposed legislation.”).

83. *Id.*

84. *Id.* at 211 (statement of Suzanne E. Spaulding); *id.* at 130 (statement of David S. Kris); *id.* at 91 (statement of James X. Dempsey, Center for Democracy and Technology).

85. The debate took place at the same time that the Intelligence Community assessed a heightened threat environment. In July 2007, the DNI released the National Intelligence Estimate (NIE) on the Terrorist Threat to the Homeland, assessing that “the US Homeland will face a persistent and evolving terrorist threat over the next three years . . . [primarily] from Islamic terrorist groups and cells, especially al-Qa’ida, driven by their undiminished intent to attack the Homeland and a continued effort by these terrorist groups to adapt and improve their capabilities.” OFFICE OF THE DIR. OF NAT’L INTELLIGENCE, NATIONAL INTELLIGENCE ESTIMATE: THE TERRORIST THREAT TO THE U.S. HOMELAND 5 (2007). The NIE is the DNI’s “most authoritative written judgment concerning national security issues . . . [and] contain[s] coordinated judgments of the Intelligence Community . . .” *Id.* at 1. The DNI also briefed Congress on the threat and the need to amend FISA in late July 2007. See 153 CONG. REC. S10,856 (daily ed. Aug. 3, 2007) (statement of Sen. Kyl) (reporting that the Intelligence Committee of the Senate had been engaged in negotiations with the DNI since he brought the matter to their attention); *id.* at S10858 (statement of Sen. Bond) (recounting that the DNI had submitted proposed reforms to FISA in April 2007 and appeared before a session of the entire Senate in the classified security area in July 2007 to urge immediate reform); S. REP. NO. 110-209, at 5 (2007) (“In late July, the DNI informed Congress that the decision of the second FISA Court judge had led to degraded capabilities in the face of a heightened terrorist threat environment. The DNI urged Congress to act prior to the August recess . . .”).

86. Administration officials later attempted to detail why these concerns were unfounded. See, e.g., *Administration Views of FISA Authorities: Hearing Before the H. Permanent Select Comm. on Intelligence*, 110th Cong. 46–52 (2007) (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_house_hearings&docid=f:38878.pdf (reiterating the positions of the Executive Branch regarding many of the concerns and misunderstandings raised by opponents of the Protect America Act); Letter from Alexander W. Joel, Civil Liberties Protection Officer, Office of the Dir. of Nat’l Intelligence, to Silvestre Reyes & Peter Hoekstra, U.S. Reps. (Sept. 17, 2007), available at <http://www.fas.org/irp/news/2007/09/joel091707.pdf> (describing civil liberties and privacy protections contained in the Protect America Act).

and personal records”⁸⁷ with “no court oversight whatsoever.”⁸⁸ Other members expressed concern about turning such power over to the Attorney General.⁸⁹ One member declared that the Protect America Act “eviscerates the Fourth Amendment to the Constitution and represents an unwarranted transfer of power from the courts to the Executive Branch.”⁹⁰

Supporters of the Protect America Act declared “unacceptable” the idea that the government should have to obtain a court order from the FISC when foreign targets communicated overseas.⁹¹ Rather, they supported returning the focus of FISA to protecting the civil liberties of U.S. persons.⁹² Some members supported the Protect America Act due to the ongoing terrorist

87. 153 CONG. REC. S10,864 (daily ed. Aug. 3, 2007) (statement of Sen. Reid). *But see id.* (statement of Sen. Levin) (“[I]f there is an incidental access to U.S. citizens, we obviously will permit that. That is not the problem. It is called minimization.”); 153 CONG. REC. H9,958 (daily ed. Aug. 4, 2007) (statement of Rep. Lungren) (“If, in the capture of this information, we do come into contact with communication that involves someone in the United States, an American citizen, we go through a process called minimization, which means we get it out of there if it has nothing to do with the evil actor.”).

88. 153 CONG. REC. S10,866 (daily ed. Aug. 3, 2007) (statement of Sen. Feingold) (stating that the “clearly erroneous” judicial review standard of the Protect America Act was “basically a standard that is nothing more than a rubberstamp”).

89. *See id.* at H9,688 (statement of Rep. Tierney) (expressing concern that authorizations of surveillance made by the Attorney General would be subject to limited court review with no apparent remedy); *id.* at H9,693 (statement of Speaker Pelosi) (stating that she would not want any attorney general, Republican or Democratic, to have the amount of power given by the Protect America Act). The Protect America Act required certification by both the Attorney General and the DNI. Protect America Act of 2007, Pub. L. No. 110-55, § 105B(a), 121 Stat. 552, 552 (to be codified at 50 U.S.C. § 1805b). Previous versions required only the certification of the Attorney General. *See* 153 CONG. REC. S10,863 (daily ed. Aug. 3, 2007) (statement of Sen. Bond) (pointing out that the requirement for DNI certification was added at the request of Admiral McConnell in light of comments from members of Congress).

90. 153 CONG. REC. H9,957 (daily ed. Aug. 4, 2007) (statement of Rep. Jackson-Lee).

91. *See* 153 CONG. REC. S10,857 (daily ed. Aug. 3, 2007) (statement of Sen. McConnell) (calling the idea that intelligence professionals might have to obtain a FISA warrant in order to conduct overseas surveillance on foreign targets “absolutely absurd and completely unacceptable”). The consensus appeared to be that foreign-to-foreign communications of non-U.S. persons fell outside of FISA. *See, e.g., id.* at S10,866 (statement of Sen. Feingold) (“Not a single Senator doesn’t think we should be able to get at these foreign calls. . . . We simply want protection for the civil liberties of people who have done absolutely nothing wrong.”); *id.* at H9,690 (statement of Rep. Conyers) (“Foreign to foreign does not require a warrant. I don’t know how many times I am going to have to say that.”). One member noted that the FISC itself believed that such matters should not be entertained by the court:

I have a very important message from the DNI: “We understand that the FISA court judges urgently support a more appropriate alignment of the court’s caseload and jurisdiction away from the focus on non-U.S. persons operating outside of the United States. The judges have clearly expressed both frustration with the fact that so much of their docket is consumed by applications that focus on foreign targets and involve minimal privacy interests of Americans.”

See id. at S10,860 (statement of Sen. Bond).

92. *See, e.g., id.* at H9,672–73 (statement of Rep. Wilson) (“We need to go back to what [FISA] was intended to do, which is to protect the civil liberties of Americans and allow us to rapidly collect foreign intelligence on foreign persons in foreign countries without first having to go to court and get a warrant.”).

threat the DNI had described to Congress, the impending congressional recess, and the six-month sunset provision.⁹³

On Friday evening, August 3, 2007, the Senate adopted S. 1927, which had been introduced by Senator McConnell, the ranking minority member, for himself and Senator Bond, the ranking SSCI member, by a vote of 60 to 28.⁹⁴ The efforts of the House of Representatives to pass a competing bill the same evening fell short.⁹⁵ The following evening, August 4, 2007 at 10:19 p.m., the House passed S. 1927 by a vote of 227 to 183.⁹⁶ Highlighting the urgency with which the Administration believed the legislation was needed, as evidenced in the DNI's public statements, President Bush immediately signed the bill on Sunday, August 5, 2007.⁹⁷

B. *Statutory Requirements*

In an attempt to change FISA to focus on the location of the target instead of the location of the surveillance or the type of communication, the Protect America Act excluded from FISA's definition of electronic surveillance "surveillance directed at a person reasonably believed to be located outside of the United States."⁹⁸ The statute granted the DNI and the Attorney General jointly the authority to "authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States" for up to one year⁹⁹ and to issue directives to communications service providers requiring them to "immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition."¹⁰⁰

93. See *id.* at S10,868 (statement of Sen. Feinstein) ("This is not going to be an easy vote for anyone. But what we have to think of right now is, on a temporary basis, how do we best protect the people of the United States against a terrible attack."); *id.* at S10,865 (statement of Sen. Lieberman) ("With all respect to my colleagues, I plead with everyone, let us not strive for perfection. Let us put national security first. Let us understand if this passes . . . we are going to have 6 months to reason together to find something better."). But see *id.* at S10,866 (statement of Sen. Feingold) ("A 6-month sunset does not justify voting for this bad version of the bill. We can't just suspend the Constitution for 6 months.").

94. BAZAN, *supra* note 3, at CRS-1 n.2. At the same time, the Senate also considered a competing bill, S. 2011, introduced by Senator Levin, Chairman of the Armed Forces Committee, on behalf of himself and Senator Rockefeller, the SSCI Chairman. S. 2011, 110th Cong. (2007). S. 2011 did not receive 60 votes, failing 43 to 45. BAZAN, *supra* note 3, at CRS-1 n.3.

95. H.R. 3356, entitled the "Improving Foreign Intelligence Surveillance to Defend the Nations and the Constitution Act of 2007," was introduced by Representative Reyes, the HPSCI Chairman, and Representative Conyers, the House Judiciary Committee Chairman, among others. BAZAN, *supra* note 3, at CRS-1. The vote on the motion to suspend House rules and pass H.R. 3356, which required a two-thirds vote instead of a majority, was 218 to 207. *Id.* at CRS-1 n.4.

96. *Id.* at CRS-1 n.5.

97. *Id.* at CRS-1.

98. Protect America Act of 2007, Pub. L. No. 110-55, § 105A, 121 Stat. 552, 552 (to be codified at 50 U.S.C. § 1805a).

99. *Id.*

100. *Id.*

To guarantee that acquisition only targeted persons outside the United States and to protect the privacy of U.S. persons, the Protect America Act required that the DNI and Attorney General certify that:

- (1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information . . . concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to [the Protect America Act];
- (2) the acquisition does not constitute electronic surveillance;
- (3) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person . . . who has access to communications, either as they are transmitted or while they are stored . . . ;
- (4) a significant purpose of the acquisition is to obtain foreign intelligence information; and
- (5) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section [1801(h) of FISA].¹⁰¹

The certification, however, was not required to “identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed.”¹⁰² The procedures were subject to the FISC’s review under a clearly erroneous standard.¹⁰³

Moreover, where a communications service provider failed to comply with a lawful directive, the Protect America Act authorized the Attorney General to move to compel compliance with the directive before the FISC.¹⁰⁴ The statute also permitted the recipient of a directive to challenge its legality before the FISC and, if the FISC did not deem the petition frivolous upon initial review, the FISC could modify or set aside the directive if the judge found that the directive did not meet the requirements of the statute or was otherwise unlawful.¹⁰⁵

101. *Id.* § 105B(a). The same section required that the certification, relying as appropriate upon affidavits of national security officials, be in writing unless immediate action was required and time did not permit the preparation of a written certification. *Id.*

102. *Id.* § 105B(b).

103. *Id.* § 105C.

104. *Id.* § 105B(g).

105. *Id.* §§ 105B(h)(1)(A)–(B). As originally enacted, portions of the Protect America Act were scheduled to sunset 180 days from the date of enactment. ELIZABETH B. BAZAN, CONG. RESEARCH SERV., THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: COMPARISON OF THE SENATE AMENDMENT TO H.R. 3773 AND THE HOUSE AMENDMENT TO THE SENATE AMENDMENT TO H.R. 3773, at 2 (2008). Congress later passed a fifteen-day extension of the Protect America Act, so those portions did not expire until February 16, 2008. *Id.* Congress subsequently enacted the FISA Amendments Act of 2008, which President Bush signed on July 10, 2008. President George W. Bush, President Bush Signs H.R. 6304, FISA Amendments Act of 2008 (July 10, 2008) (transcript available at <http://georgewbush-whitehouse.archives.gov/news/releases/2008/07/>)

IV. The Court of Review Decision

The Court of Review in *In re Directives* did not write on a blank slate. Indeed, the decision is consistent with legal precedent regarding the Executive Branch's acquisition of foreign intelligence information in a manner consistent with the requirements of the Fourth Amendment.¹⁰⁶ First, the Court of Review held that a foreign intelligence exception to the Warrant Clause exists, at a minimum, in the limited circumstances outlined below.¹⁰⁷ Second, the court held that the warrantless surveillance comports with the Fourth Amendment's reasonableness requirement, even where the surveillance acquires communications of a U.S. person who is not a target of the surveillance.¹⁰⁸ The two holdings are significant for their clarity and because they answered constitutional questions regarding the Executive Branch's authority to conduct certain surveillance without prior judicial review so soon after that very issue was debated before Congress.

A. *The Directives and a Summary of the Provider's Challenge*

In 2007, the government issued directives to the provider.¹⁰⁹ The directives required the provider to assist the government in its acquisition of foreign intelligence information through the warrantless surveillance of certain of the provider's customers reasonably believed to be located outside the United States.¹¹⁰

The directives were issued pursuant to Protect America Act certifications.¹¹¹ At least on the face of the statute, the directives lacked key attributes of a traditional warrant. They were issued without a particularity requirement and a requirement for prior judicial review for determining probable cause.¹¹² Those certifications, however, contained protections beyond those specified by the statute, namely the requirement that the Attorney

20080710-2.html). For a discussion of congressional action between August 2007 and July 2008, see generally BAZAN, *supra*.

106. See *infra* notes 132–36 and accompanying text.

107. See *In re Directives*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (“[W]e hold that a foreign intelligence exception to the Fourth Amendment’s warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.”).

108. *Id.* at 1013, 1015.

109. *Id.* at 1007.

110. *Id.* at 1006–07.

111. *Id.* at 1007.

112. See *id.* at 1013–14 (noting that the Protect America Act lacks a particularity requirement and a prior judicial review requirement for determining probable cause, protections equivalent to the principal warrant requirements); Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 552–55 (to be codified at 50 U.S.C. §§ 1805a, 1805b) (listing the requirements to which the DNI and Attorney General must certify as well as indicating that the DNI and Attorney General may direct a person to “immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition”). For a fuller discussion of the Court of Review’s consideration of prior judicial review, see *infra* text accompanying notes 196–209.

General and the NSA follow procedures implemented pursuant to § 2.5 of Executive Order 12,333, as amended.¹¹³ Section 2.5 of Executive Order 12,333 provides that the Attorney General may authorize surveillance of U.S. persons only when the Attorney General has “determined in each case that there is probable cause to believe that the [surveillance] technique is directed against a foreign power or an agent of a foreign power.”¹¹⁴ In addition, the certifications contained procedures designed to direct any authorized surveillance against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.¹¹⁵

The provider refused to comply with the directives.¹¹⁶ Pursuant to § 105B(g) of the Protect America Act, the Government moved the FISC for an order compelling the provider’s compliance.¹¹⁷ After “amplitudinous” briefing, the FISC issued a “meticulous” opinion validating the directives and granting the motion to compel.¹¹⁸ The provider then filed a petition for review with the Court of Review and moved the FISC for a stay pending its appeal.¹¹⁹ When the FISC denied the motion for a stay and threatened to hold the provider in civil contempt, the provider began compliance with the directives.¹²⁰

The provider continued to comply throughout the proceedings before the Court of Review.¹²¹ On August 22, 2008, following oral argument on the merits, the Court of Review issued a classified opinion that affirmed the FISC’s decision that the directives were lawful and that compliance was

113. *In re Directives*, 551 F.3d at 1007. Because the Protect America Act did not distinguish between U.S. persons and non-U.S. persons, the government was being more restrictive than the statute by applying § 2.5 to the certifications. *See supra* note 60 (indicating that § 2.5 authorized surveillance only “within the United States or against a United States person abroad”); *infra* text accompanying note 126 (relating that the Protect America Act authorized surveillance of persons reasonably believed to be outside the United States, without regard to U.S.-person status).

114. Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008), *reprinted as amended in* 50 U.S.C. § 401 (2006).

115. *In re Directives*, 551 F.3d at 1007–08. The FISC found the government’s procedures implementing the statute sufficient under the Protect America Act. *See* NSD PROGRESS REPORT, *supra* note 66, at 21 (“On January 15, 2008, the FISA Court, after reviewing the Government’s submissions, issued an order upholding the procedures the Government uses to determine that targets subject to surveillance under this authority are reasonably believed to be abroad.”); *see also In re Directives*, 551 F.3d at 1015 (noting that “[t]hese minimization procedures were upheld by the FISC in this case”).

116. *In re Directives*, 551 F.3d at 1008.

117. *Id.*

118. *Id.*

119. *Id.*

120. *Id.* The provider also moved the Court of Review for a stay pending appeal. *Id.* The Court of Review reserved decision on the motion for a stay, and the provider continued its compliance with the directives. *Id.* As part of its opinion upholding the lawfulness of the directives, the Court of Review denied the motion for a stay as moot. *Id.* at 1016.

121. *Id.* at 1008.

required.¹²² By order dated January 12, 2009, the Court of Review issued a redacted, unclassified version of its opinion.¹²³

B. The Limited Scope of the Fourth Amendment Claim

The provider's Fourth Amendment arguments were limited in terms of the persons whose interests it sought to vindicate.¹²⁴ The provider challenged the directives only in regard to the Fourth Amendment rights of U.S. persons.¹²⁵ The statute, however, had a broader application. The statute authorized surveillance of persons reasonably believed to be outside the United States, without regard to U.S.-person status.¹²⁶ To the extent targets were non-U.S. persons, however, the statute and any directives thereunder did not implicate the Fourth Amendment because the Fourth Amendment does not apply to searches of non-U.S. persons located outside the United States.¹²⁷ The constitutional challenge accordingly focused on the Fourth Amendment rights of two categories of U.S. persons: U.S. persons abroad who were the targets of surveillance and U.S. persons whose

122. *Id.* at 1004, 1008, 1016.

123. *Id.* at 1016–18.

124. Before reaching the merits of the Fourth Amendment claim, the Court of Review addressed the Government's argument that the provider lacked standing to challenge the legality of the directives on behalf of its customers. Specifically, the Government had argued that the provider's claim was contrary to the rule that a litigant cannot bring suit to vindicate the rights of third parties. *See id.* at 1008 (citing *Hinck v. United States*, 550 U.S. 501, 510 n.3 (2007), and *Warth v. Seldin*, 422 U.S. 490, 499 (1975), for the rule that a litigant must assert his own legal rights, not those of third parties); *see also* *Cal. Bankers Ass'n v. Schultz*, 416 U.S. 21, 69–70 (1974) (refusing to consider a bank's claim that certain federal reporting requirements violated the Fourth Amendment rights of non-party bank customers "whose transactions must be reported" under federal law); *Alderman v. United States*, 394 U.S. 165, 174 (1969) ("Fourth Amendment rights are personal rights which . . . may not be vicariously asserted."); *Hollingsworth v. Hill*, 110 F.3d 733, 738 (10th Cir. 1997) (holding that a mother could not challenge seizure of her minor children on the ground that it violated her children's Fourth Amendment rights because her complaint did not include the children as plaintiffs); *Ellwest Stereo Theatres, Inc. v. Wenner*, 681 F.2d 1243, 1248 (9th Cir. 1982) (rejecting an adult theater's challenge to a city ordinance on the ground that any police surveillance enabled by the ordinance did not threaten the theater's Fourth Amendment interests, but only "the interests of its patrons"). The Court of Review held that the provider "easily exceed[ed] the constitutional threshold for standing." *In re Directives*, 551 F.3d at 1008. Furthermore, it held that any prudential standing limitation was relaxed by the terms of the Protect America Act, which expressly placed no limits on the types of claims a provider could bring. *See id.* at 1008–09 ("We think that the language is broad enough to permit a service provider to bring a constitutional challenge to the legality of a directive regardless of whether the provider or one of its customers suffers the infringement that makes the directive unlawful.").

125. *In re Directives*, 551 F.3d at 1009.

126. Protect America Act of 2007, Pub. L. No. 110-55, § 2, 121 Stat. 552, 552–55 (to be codified at 50 U.S.C. §§ 1805a, 1805b).

127. *See* *United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990) (holding that only those persons who "have come within the territory of the United States and developed substantial connections" with the country have Fourth Amendment rights).

communications were collected incidentally by the government while targeting individuals abroad.¹²⁸

In the context of these limits, the provider advanced two Fourth Amendment arguments. First, it argued that the Fourth Amendment's Warrant Clause applied to the surveillance and that the directives were unlawful because they were not warrants.¹²⁹ Second, the provider argued that even if the Warrant Clause did not apply, the surveillance failed to satisfy the Fourth Amendment's reasonableness requirement.¹³⁰ The court rejected each of these arguments.¹³¹

1. *A Clear Holding: Foreign Intelligence Collection Is a Special Need Excusing Compliance with the Warrant Clause.*—Prior case law provided little support for the provider's argument that the Warrant Clause applied to the type of foreign intelligence surveillance authorized by the Protect America Act. Every court of appeals to decide the question had held that the Fourth Amendment does not require the government to obtain a judicial warrant before conducting a foreign intelligence search.¹³² Many, if not all, of

128. See *In re Directives*, 551 F.3d at 1009 (relating that the petitioner's claims were limited to the harm that may be inflicted upon U.S. persons); *id.* at 1014 (explaining that § 2.5 of Executive Order 12,333, which the government applied to the certifications, authorizes surveillance "within the United States or against a United States person abroad"); *id.* at 1015 (referencing the implemented minimization procedures, which aimed at "reducing the impact of incidental intrusions into the privacy of non-targeted United States persons"). The Court of Review also limited its analysis of the claim to the particularized fact record before it. *Id.* at 1010. The provider had argued that its challenge was a facial challenge to the statute. *Id.* at 1009. Under a facial challenge analysis, a court considers the constitutionality of a statute without regard to facts describing the government's particular application of the statute. *Id.* The Court of Review held that the challenge, in fact, was an as-applied challenge and not a facial challenge. *Id.* at 1009–10. There was a particularized record, the statute was applied to the provider in a specific setting, and the provider's arguments took account of that setting. *Id.* at 1009. "So viewed, [the arguments] go past the question of whether the [Protect America Act] is valid on its face—a question that would be answered by deciding whether *any* application of the statute passed constitutional muster . . .—and ask instead whether this specific application offends the Constitution." *Id.* at 1009–10 (citing *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 449 (2008)). Because the court conducted an as-applied analysis, it considered, among other things, the extra-statutory privacy protections implemented through the certifications and directives. See *In re Directives*, 551 F.3d at 1013–14 (considering the Protect America Act as applied here, including "the protections spelled out in the [Act] itself and those mandated under the certifications and directives").

129. *In re Directives*, 551 F.3d at 1009.

130. *Id.*

131. *Id.* at 1010–12.

132. See *United States v. Truong Dinh Hung*, 629 F.2d 908, 912–16 (4th Cir. 1980) (upholding warrantless foreign intelligence surveillance authorized by the Attorney General); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) ("Foreign security wiretaps are a recognized exception to the general warrant requirement . . ."); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir. 1974) (upholding warrantless foreign intelligence surveillance and relying on the "good faith of the Executive and the sanctions for illegal surveillances incident to post-search criminal or civil litigation"); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973) ("[B]ecause of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs . . . the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence.");

these cases involved surveillance inside the United States.¹³³ If, as they held, there was an exception to the Warrant Clause for the collection of foreign intelligence information from persons inside the United States, then this foreign intelligence exception applied *a fortiori* to acquisitions pursuant to the Protect America Act that were directed at persons reasonably believed to be outside the United States.

The Court of Review, in *In re Sealed Case*,¹³⁴ itself recognized a foreign intelligence exception to the warrant requirement.¹³⁵ In that case, the Court of Review held that surveillance for foreign intelligence information under FISA complied with the Fourth Amendment without determining whether an electronic surveillance order under 50 U.S.C. § 1805 constituted a “warrant” within the meaning of the Warrant Clause.¹³⁶ Although it avoided an express holding that a foreign intelligence exception exists, such a holding was implicit: had the Warrant Clause applied, the Court of Review would have had to have determined whether a FISA electronic surveillance order was a warrant. Because it upheld the lawfulness of the electronic surveillance order on Fourth Amendment reasonableness grounds without the warrant determination, the court implicitly held that no warrant was required.¹³⁷

In *In re Directives*, however, the court’s holding was express:

[W]e hold that a foreign intelligence exception to the Fourth Amendment’s warrant requirement exists when the surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.¹³⁸

see also In re Sealed Case, 310 F.3d 717, 742 (FISA Ct. Rev. 2002) (“[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information.”). In *Zweibon v. Mitchell*, 516 F.2d 594, 633–51 (D.C. Cir. 1975) (en banc) (plurality opinion), a plurality of the D.C. Circuit suggested that a warrant might be required to conduct surveillance for foreign intelligence purposes, but this suggestion was dicta. *See In re Sealed Case*, 310 F.3d at 742 n.26 (noting that in regard to a foreign intelligence exception to the warrant requirement, *Zweibon* “suggested the contrary in dicta, it did not decide the issue”).

133. *See, e.g., Truong*, 629 F.2d at 912 (involving eavesdropping on telephone conversations and bugging an apartment in the United States); *Buck*, 548 F.2d at 874 (relating to electronic surveillance in the United States); *Butenko*, 494 F.2d at 596 (discussing “the relationship between the federal government’s need to accumulate information concerning activities within the United States of foreign powers and the people’s right of privacy as embodied in the Fourth Amendment”); *Brown*, 484 F.2d at 426 (concluding that wiretaps conducted in the United States were lawful).

134. 310 F.3d at 717.

135. *Id.* at 741–42.

136. *Id.* at 742.

137. *See id.* at 741–42 (noting that “a FISA order may not be a ‘warrant’ contemplated by the Fourth Amendment” and remarking that the “government itself does not actually claim that it is, instead noting only that there is authority for the proposition that a FISA order is a warrant in the constitutional sense”).

138. *In re Directives*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008).

The court, furthermore, based its holding on Fourth Amendment principles developed outside the context of foreign intelligence surveillance.¹³⁹

Although the Supreme Court had not expressly recognized an exception to the Warrant Clause for foreign intelligence surveillance,¹⁴⁰ it had issued a relevant body of decisions referred to as “special needs” cases.¹⁴¹ As the Court of Review noted, those cases “excused compliance with the Warrant Clause when the purpose behind the governmental action went beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose.”¹⁴² The Court of Review held that the reasoning of the special needs cases applied to justify an exception to the warrant requirement for surveillance pursuant to the Protect America Act.¹⁴³

The threshold consideration in the special needs cases is whether a search was designed to uncover evidence of “ordinary criminal wrongdoing” or was motivated “at [a] programmatic level” by other governmental objectives.¹⁴⁴ The Court of Review held that Protect America Act

139. *Id.* at 1010–12.

140. The Supreme Court in *Keith* expressly reserved the question of whether the Fourth Amendment required a warrant for foreign intelligence surveillance, but in so doing suggested possible parameters for such an exception. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 321–22 (1972) (“As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues that may be involved with respect to activities of foreign powers or their agents.”). In concluding that the Fourth Amendment’s warrant requirement applies to investigation of purely domestic threats to security, the *Keith* Court discussed several sources supporting “the view that warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved.” *Id.* at 322 n.20; *see also Katz v. United States*, 389 U.S. 347, 358 n.23 (1967) (“Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.”).

141. *In re Directives*, 551 F.3d at 1010.

142. *Id.* (citations omitted).

143. *Id.* at 1011.

144. *City of Indianapolis v. Edmond*, 531 U.S. 32, 37–40, 48 (2000); *see also In re Directives*, 551 F.3d at 1011 (“In our view the more appropriate consideration is the programmatic purpose of the surveillances and whether—as in the special needs cases—that programmatic purpose involves some legitimate objective beyond ordinary crime control.”). Accordingly, the Supreme Court has permitted, *inter alia*, the following: warrantless stops of motorists at roadblocks for the purpose of securing the border, *see United States v. Martinez-Fuerte*, 428 U.S. 543, 566 (1976) (holding that vehicle stops at fixed checkpoints for brief questioning of the occupants, even though there is not reason to believe a particular vehicle contains illegal aliens, are consistent with the Fourth Amendment and need not be authorized by warrant); warrantless searches of the homes of persons on probation to ensure compliance with probation conditions, *see Griffin v. Wisconsin*, 483 U.S. 866, 872–73 (1987) (holding that the search of a home satisfied the demands of the Fourth Amendment because it was carried out pursuant to a regulation that itself satisfied the Fourth Amendment’s reasonableness requirement); and warrantless searches of public school students in order to enforce school rules, *see New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (noting that the “fundamental command of the Fourth Amendment is that searches and seizures be reasonable, and although ‘both the concept of probable cause and the requirement of a warrant bear on the reasonableness of a search, . . . in certain limited circumstances neither is required’”). The Supreme Court has also approved warrantless and suspicionless drug testing of the following groups: students

surveillances had a programmatic purpose “well beyond any garden-variety law enforcement objective,” and “easily pass muster” in this regard.¹⁴⁵ This conclusion was consistent with the decision in *In re Sealed Case*.¹⁴⁶ The programmatic purpose of surveillance approved in that case was fundamentally the same as the programmatic purpose of surveillance authorized by the directives: the acquisition of foreign intelligence information to protect against threats to national security directed by foreign powers and their agents.¹⁴⁷ In support of this conclusion, the Court of Review found that the “stated purpose” of the directives “centers on garnering foreign intelligence.”¹⁴⁸ The court also observed that there was “no indication that

involved in extracurricular activities, *see* *Bd. of Educ. v. Earls*, 536 U.S. 822, 829–38 (2002) (holding that a policy requiring all students who participate in competitive extracurricular activities submit to drug testing was a reasonable means of furthering the school district’s interest in thwarting and discouraging drug use among students and therefore did not violate the Fourth Amendment); students involved in school athletics, *see* *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 664–65 (1995) (upholding drug testing of high school athletes and explaining that the exception to the warrant requirement applied when special needs that are beyond the normal need for law enforcement make the warrant and probable cause requirements unworkable); federal employees charged with enforcing drug laws or carrying firearms, *see* *Nat’l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 679 (1989) (holding that when the government requires its employees to produce urine samples to be analyzed for illegal drug use, the collection and analysis of such samples are searches that meet the reasonableness requirement of the Fourth Amendment); and railroad employees whose job functions implicate safety concerns, *see* *Skinner v. Ry. Labor Executives’ Ass’n*, 489 U.S. 602, 624 (1989) (upholding regulations instituting drug and alcohol testing of railroad workers for safety reasons).

145. *In re Directives*, 551 F.3d at 1011.

146. Courts in similar cases have held that searches to protect against threats to national security qualify for the special needs exception to the warrant requirement. *See* *Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006) (“[T]he prevention of terrorist attacks . . . constitutes a ‘special need’ Preventing or deterring large-scale terrorist attacks present problems that are distinct from standard law enforcement needs and indeed go well beyond them.”); *MacWade v. Kelly*, 460 F.3d 260, 271 (2d Cir. 2006) (“[P]reventing a terrorist from bombing the subways constitutes a special need that is distinct from ordinary post hoc criminal investigation.”).

147. *Compare* *In re Directives*, 551 F.3d at 1011 (finding that surveillances authorized by directives involve “the acquisition from overseas agents of foreign intelligence to help protect national security”), *with* *In re Sealed Case*, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) (holding that the programmatic purpose was “to protect the nation against terrorists and espionage threats directed by foreign powers”).

148. *In re Directives*, 551 F.3d at 1011. The debate regarding the Protect America Act included concerns that, without more oversight, the government would use the statute’s authorities for purposes other than those authorized by the statute. *See* *Modernization of FISA*, *supra* note 7, at 44 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. for National Security, United States Department of Justice). The Court of Review did not entertain such arguments, instead presuming that the government acted as it stated. *See* *In re Directives*, 551 F.3d at 1011 (“Without something more than a purely speculative set of imaginings, we cannot infer that the purpose of the directives (and, thus, of the surveillances) is other than their stated purpose.”). *See, e.g.*, *United States v. Chem. Found., Inc.*, 272 U.S. 1, 14–15 (1926) (“The presumption of regularity supports the official acts of public officers, and, in the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties.” (internal citations omitted)).

the collections of information [were] primarily related to ordinary criminal-law enforcement purposes.”¹⁴⁹

Next, the Court of Review held that that the Protect America Act surveillance satisfied the second consideration for a special needs exception: a warrant requirement would “materially interfere with the accomplishment of” the programmatic purpose.¹⁵⁰ The Government’s proof on this point was bolstered by congressional findings.¹⁵¹ Congress passed the Protect America Act precisely because the burden of preparing FISA applications was harming the government’s ability to collect foreign intelligence information from targets overseas.¹⁵² Citing classified information that was redacted from the published opinion and not given to the provider in the litigation, the court held that “there is a high degree of probability that requiring a warrant would hinder the government’s ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake.”¹⁵³ In addition, the court held that “[c]ompulsory compliance with the warrant requirement would introduce an element of delay, thus frustrating the government’s ability to collect information in a timely manner.”¹⁵⁴

2. *Warrantless Collection of U.S.-Person Communications Is Reasonable Under the Fourth Amendment.*—Although the Government established a special-needs exception to the Warrant Clause for its foreign intelligence surveillance, the Fourth Amendment still required that the surveillance be reasonable. As the Court of Review noted, “the question here

149. *In re Directives*, 551 F.3d at 1011. The provider argued that the government could not invoke a foreign intelligence exception unless the primary purpose of the search was the collection of foreign intelligence. The Court of Review, however, had rejected the “primary purpose” test in *In re Sealed Case* as being inconsistent with special needs case law and its programmatic purpose analysis. Citing its holding in *In re Sealed Case*, the Court of Review rejected the provider’s argument on the same grounds. *See id.* (“That dog will not hunt.”).

150. *Id.* at 1010.

151. *Id.* at 1008–09.

152. *See, e.g.*, 153 CONG. REC. S10,857 (daily ed. Aug. 3, 2007) (statement of Sen. McConnell) (stating that the legislation’s purpose is to provide the government with “the speed and the flexibility” to “collect foreign intelligence concerning foreign targets overseas in another country”).

153. *In re Directives*, 551 F.3d at 1011 (citations omitted). In describing the compelling needs of the Executive in foreign intelligence gathering, the *Truong* court observed,

[A]ttempts to counter foreign threats to the national security require utmost stealth, speed, and secrecy. A warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations.

United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980); *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 273 (S.D.N.Y. 2000) (finding that “the imposition of a warrant requirement [would] be a disproportionate and perhaps even disabling burden” on the government’s ability to obtain foreign intelligence information effectively); *cf. In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157, 171 (2d Cir. 2008) (“[W]e hold that the Fourth Amendment’s Warrant Clause has no extraterritorial application and that foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment’s requirement of reasonableness.”).

154. *In re Directives*, 551 F.3d at 1011–12.

reduces to whether the [statute], as applied through the directives, constitutes a sufficiently reasonable exercise of governmental power to satisfy the Fourth Amendment."¹⁵⁵

In evaluating reasonableness, the Court of Review invoked well-settled Fourth Amendment standards. Reasonableness would be determined based on the totality of the circumstances, balancing the interests at stake.¹⁵⁶ This analysis would account for the nature of the government intrusion and how the intrusion is implemented.¹⁵⁷ The greater the government interest, the greater the intrusion that may be tolerated.¹⁵⁸ If, based on these considerations, "the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake," the court would uphold the surveillance as constitutional.¹⁵⁹ If, however, "those protections are insufficient to alleviate the risks of government error and abuse," the court would find the surveillance to be unconstitutional.¹⁶⁰

In terms of the government's interest in the surveillance, there was little debate: the government had put forth an interest "of the highest order of magnitude," the interest in national security.¹⁶¹ Under the reasonableness standards set forth by the Court of Review, this "important interest" in national security could justify a greater intrusion in individual privacy.¹⁶² But before it considered the relative merits of those protections, the court revisited its *In re Sealed Case* decision to respond to the provider's arguments about what *In re Sealed Case* did and did not say about the application of the totality-of-circumstances test and the reasonableness of foreign intelligence surveillance.¹⁶³

The provider argued that the totality-of-circumstances test required consideration of certain specific factors.¹⁶⁴ It first argued that the court must consider the six factors that *In re Sealed Case* found contributed to the protection of individual privacy in the face of government intrusion for national security purposes—prior judicial review, presence or absence of probable cause, particularity, necessity, limited duration, and minimization.¹⁶⁵ As a related point, the provider next argued that *In re*

155. *Id.* at 1012.

156. *Id.*

157. *Id.*

158. *Id.*

159. *Id.*

160. *Id.*

161. *Id.* at 1012 (citing *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." (internal citations omitted)) and *In re Sealed Case*, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) (holding that the national security threat at issue "may well involve the most serious threat our country faces")).

162. *Id.* at 1012 (citing *Michigan v. Summers*, 452 U.S. 692, 701–05 (1981)).

163. *Id.* at 1012–13.

164. *Id.* at 1012.

165. *Id.*

Sealed Case required that surveillance pursuant to the directives must contain procedures equivalent to the three principal warrant requirements, namely prior judicial review, probable cause, and particularity.¹⁶⁶

The Court of Review summarily rejected these arguments. It held that *In re Sealed Case* did not formulate a “rigid six-factor test for reasonableness.”¹⁶⁷ Such a test “would be at odds with the totality of the circumstances test,”¹⁶⁸ and, in any event, *In re Sealed Case* “merely indicated that the six enumerated factors were relevant under the circumstances of that case.”¹⁶⁹

In re Sealed Case was clear on this point: the procedures it considered in evaluating the reasonableness of FISA surveillance—procedures required by Title III for ordinary criminal warrants—were “not constitutionally required.”¹⁷⁰ The Court of Review looked instead to such procedures as “instructive” to its reasonableness analysis, recognizing that reasonableness depends on the “facts and circumstances of each case.”¹⁷¹ Given FISA’s resemblance to a traditional warrant regime, it made sense for the Court of Review in *In re Sealed Case* to compare FISA to the Title III procedures in assessing reasonableness.¹⁷² But the Court of Review did not hold that such procedures were constitutionally required. Rather, it weighed such procedures, among many other factors, in its assessment of the reasonableness of the FISC orders under the Fourth Amendment.¹⁷³

The Court of Review also rejected the provider’s argument that directives must contain protections equivalent to the three principal warrant clause requirements of prior judicial review, probable cause, and particularity.¹⁷⁴ This argument, the court held, was essentially an attempt to impose a warrant requirement on foreign intelligence surveillance that it had determined was exempt from just such a requirement.¹⁷⁵ The argument also misread *In re Sealed Case*. These three warrant requirements were relevant to a reasonableness analysis—“the more a set of procedures resembles those associated with the traditional warrant requirements, the more easily it can be determined that those procedures are within constitutional bounds”—but they

166. *Id.* at 1013.

167. *Id.* at 1012.

168. *Id.* at 1012–13. Indeed, the determination whether a search is reasonable “requires careful attention to the facts and circumstances of each particular case.” *Graham v. Connor*, 490 U.S. 386, 396 (1989); *see also* *United States v. Redmon*, 138 F.3d 1109, 1128 (7th Cir. 1998) (Flaum, J., concurring) (“No one factor can be a talismanic indicator of reasonableness . . .”).

169. *In re Directives*, 551 F.3d at 1013.

170. *In re Sealed Case*, 310 F.3d 717, 737 (FISA Ct. Rev. 2002).

171. *Id.* at 737, 740.

172. *See id.* at 737–42 (detailing the similarities between FISA and Title III and noting that how closely a FISA order complies with Title III bears on the reasonableness analysis under the Fourth Amendment).

173. *Id.*

174. *In re Directives*, 551 F.3d at 1013.

175. *Id.*

were not of themselves determinative.¹⁷⁶ Consistent with Fourth Amendment case law, the guiding principle would be the totality of the circumstances, and not some limited set of circumstances.¹⁷⁷

Based on the totality of circumstances, the Court of Review held that the directives constituted reasonable government action.¹⁷⁸ The Protect America Act, the certifications, and the directives contained a “matrix of safeguards.”¹⁷⁹ The provider offered only a “parade of horrors” concerning these safeguards, but no evidence that, notwithstanding the safeguards, there was “any actual harm, any egregious risk of error, or any broad potential for abuse”¹⁸⁰ Thus, in light of the important government interest in national security and the “panoply of protections,” the court held that there was “no principled basis for invalidating the [Protect America Act] as applied here.”¹⁸¹

To reach its reasonableness conclusion, the Court of Review focused on the issues of particularity, probable cause, prior judicial review, and the incidental collection of information from non-targeted U.S. persons.¹⁸² With respect to particularity, the Protect America Act did not require a showing of particularity.¹⁸³ Although required by the Warrant Clause,¹⁸⁴ particularity in the context of warrantless searches is but one factor among many in assessing reasonableness.¹⁸⁵ The Court of Review held that the surveillance authorized by the directives sufficiently addressed any particularity considerations.¹⁸⁶ It did so by analogy to FISA electronic surveillance, which it had held was reasonable in *In re Sealed Case*.¹⁸⁷ FISA’s electronic surveillance provisions require probable cause to believe that the facility or place at which surveillance is directed is being used, or about to be used, by an agent of a foreign power.¹⁸⁸ In the case before it, the Court of Review found that

176. See *id.* (declining to incorporate warrant requirements into the foreign intelligence exception of the Fourth Amendment).

177. *Id.*

178. *Id.*

179. *Id.*

180. *Id.*

181. *Id.*

182. *Id.* at 1013–14.

183. *Id.* at 1013 (citing 50 U.S.C. § 1805b(b) (Supp. I 2007–2008)).

184. See U.S. CONST. amend. IV (“[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched.*” (emphasis added)).

185. See *United States v. Martinez-Fuerte*, 428 U.S. 543, 561 (1976) (proclaiming that “the Fourth Amendment imposes no irreducible requirement” of individualized findings where the search in question is otherwise reasonable).

186. *In re Directives*, 551 F.3d at 1013–14.

187. *Id.*

188. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 104, 92 Stat. 1783, 1789 (codified at 50 U.S.C. § 1805(a)(3)(B) (2006)).

certain classified procedures were “analogous to and in conformity with the particularity showing contemplated by *Sealed Case*.”¹⁸⁹

The Court of Review held that any probable cause concern was allayed by the Attorney General’s findings made pursuant to § 2.5 of Executive Order 12,333, made applicable to the surveillances through the certifications and directives.¹⁹⁰ Section 2.5 authorizes the Attorney General to approve “the use for intelligence purposes . . . against a U.S. person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes . . .”¹⁹¹ The Attorney General may authorize such surveillance only when he “determine[s] in each case that there is *probable cause* to believe that the [surveillance] technique is directed against a *foreign power or an agent of a foreign power*.”¹⁹² As applied to Protect America Act surveillance, the court found that, before the government could act upon the certifications, the Attorney General must determine that there was probable cause to believe that the targeted U.S. person was a foreign power or agent of a foreign power.¹⁹³ This determination was supported by, among other information, a several-page statement of facts provided by the NSA in support of the probable cause determination.¹⁹⁴

Harkening back to the debate concerning the Protect America Act,¹⁹⁵ the provider also argued that the directives were unreasonable because, without prior judicial review, they “cede to [the Executive] Branch overly broad power that invites abuse.”¹⁹⁶ The Court of Review described this argument as “little more than a lament about the risk that government officials will not operate in good faith.”¹⁹⁷ A prior judicial review requirement does not eliminate that risk—it “exists even when a warrant is required.”¹⁹⁸ Despite the risk of fraud or misconduct by a warrant affiant, courts traditionally apply a presumption of regularity to the obtaining of a warrant, unless there is a showing of actual fraud or misconduct.¹⁹⁹ In the same way, the Court of Review applied a presumption of regularity to the Executive Branch’s decision to authorize surveillance.²⁰⁰ It analyzed whether the government

189. See *In re Directives*, 551 F.3d at 1013–14 (noting that the classified procedures were part of an *ex parte* appendix filed by the Government and not disclosed to petitioner).

190. *Id.* at 1014.

191. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 8, 1981).

192. *Id.* (emphasis added).

193. *In re Directives*, 551 F.3d at 1014.

194. *Id.* at 1014 n.7; see also *supra* note 60.

195. See 153 CONG. REC. H9,957 (daily ed. Aug. 4, 2007) (statement of Rep. Jackson-Lee) (lamenting the Protect America Act’s “unwarranted transfer of power from the courts to the Executive Branch”).

196. *In re Directives*, 551 F.3d at 1014.

197. *Id.*

198. *Id.*

199. *Id.*

200. See *id.* (“Here—where an exception affords relief from the warrant requirement—common sense suggests that we import the same presumption.”).

had put in place protections and procedures sufficient to satisfy the Fourth Amendment's reasonableness requirement.²⁰¹ Once the Court of Review determined that those protections and procedures were sufficient, it would not assume that the government would implement them in bad faith, absent evidence to that effect.²⁰²

The court had applied the same presumption of regularity when evaluating the government's programmatic purpose for a special-needs exception to the Warrant Clause. In that context, the provider's "purely speculative set of imaginings" were no basis to question the government's stated, programmatic purpose.²⁰³ Likewise, in the context of evaluating the Fourth Amendment reasonableness of the government's procedures, the provider's "parade of horrors" did not undermine otherwise reasonable procedures.²⁰⁴

Prior judicial review, moreover, did not ensure against the risk of inadvertent collection, and in general, the "potential for error is not a sufficient reason to invalidate the surveillances."²⁰⁵ The court noted that the government had put in place "effective minimization procedures" that serve as "an additional backstop against identification errors."²⁰⁶ Those minimization procedures were "almost identical to those used under FISA to ensure the curtailment of both mistaken and incidental acquisitions," were approved by the FISC in the case below,²⁰⁷ and were approved in the FISA context by the Court of Review in *In re Sealed Case*.²⁰⁸ The court, accordingly, held that it saw "no reason to question the adequacy of the minimization protocol."²⁰⁹

The court also addressed the provider's arguments regarding the incidental collection of U.S. person communications—that is, the collection of communications of U.S. persons who are not targeted for surveillance but who are in communication with targeted persons reasonably believed to be located outside the United States.²¹⁰ This holding goes to the heart of the debate on the Protect America Act. As noted above, even critics of the Protect America Act did not dispute that FISA should not cover foreign-to-foreign communications by non-U.S. persons.²¹¹ Rather, they were concerned about the collection of U.S.-person communications being sucked up

201. *Id.* at 1014–15.

202. *Id.*

203. *Id.* at 1011.

204. *Id.* at 1013.

205. *Id.* at 1014–15; *see also* *Pasiewicz v. Lake County Forest Pres. Dist.*, 270 F.3d 520, 525 (7th Cir. 2001) (“[T]he Fourth Amendment demands reasonableness, not perfection.”).

206. *In re Directives*, 551 F.3d at 1015.

207. *Id.*

208. 310 F.2d 717, 731 (FISA Ct. Rev. 2002).

209. *In re Directives*, 551 F.3d at 1015.

210. *Id.*

211. *See supra* notes 83–84 and accompanying text.

in NSA's so-called "vacuum cleaner."²¹² The court held that the provider's "concern with incidental collections is overblown."²¹³ According to the Court of Review, "[i]t is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."²¹⁴ This conclusion applies fully to surveillance for the purpose of collecting foreign intelligence.²¹⁵

The directives, in any event, extended certain protections to U.S. persons whose communications were incidentally collected. The Court of Review noted two such protections in particular: targeting procedures and minimization procedures.²¹⁶ The targeting procedures "include provisions to prevent errors" and the Protect America Act provides for both Executive Branch and congressional oversight of compliance with the targeting procedures.²¹⁷ Minimization procedures, which the court described as "effective," also protected those impacted by incidental collection.²¹⁸ As noted by the court, minimization procedures serve "as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons."²¹⁹ Together, these protections for U.S. persons whose

212. James X. Dempsey of the Center for Democracy Technology (CDT) stated to Congress that the term "vacuum cleaner" was appropriate because the Protect America Act "would permit [the NSA] without a warrant the untargeted collection of many, many calls, without the particularized suspicion required by the Constitution for government searches," but also added that "the CDT has been on the record supporting an amendment to FISA that would make it clear that a warrant is not needed when the government is intercepting foreign-to-foreign communications that happen to be available in the U.S." *Modernization of FISA*, *supra* note 7, at 88–91 (statement of James X. Dempsey, Policy Director, Center for Democracy and Technology).

213. *In re Directives*, 551 F.3d at 1015; *see also supra* note 87 (statement of Sen. Levin).

214. *In re Directives*, 551 F.3d at 1015 (citing *United States v. Kahn*, 415 U.S. 143, 157–58 (1974) (holding that the interception of a wife's communications incident to the lawful wiretap of a home phone targeting her husband's communications did not violate the Fourth Amendment) and *United States v. Schwartz*, 535 F.2d 160, 164 (2d Cir. 1976) ("It is virtually impossible to completely exclude all irrelevant matter from intercepted conversations."); *see also United States v. Figueroa*, 757 F.2d 466, 472–73 (2d Cir. 1985) ("[A] wiretap order which does not specify every person whose conversations may be intercepted does not *per se* amount to a 'virtual general warrant' in violation of the fourth amendment."); *United States v. Tortorello*, 480 F.2d 764, 775 (2d Cir. 1973) (holding that once the relevant authority for the search has been established as to one participant, the statements of other, incidental "participants may be intercepted if pertinent to the investigation").

215. *See United States v. Butenko*, 494 F.2d 593, 608 (3d Cir. 1974) ("To be sure, in the course of such wiretapping conversations of alien officials and agents, and perhaps of American citizens, will be overheard and to that extent, their privacy infringed. But the Fourth Amendment proscribes only 'unreasonable' searches and seizures."); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) ("[I]ncidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment.")

216. *In re Directives*, 551 F.3d at 1015.

217. *Id.*

218. *Id.*

219. *Id.* FISA's definition of minimization procedures, incorporated by the Protect America Act, includes procedures that require that non-publicly available information that is not foreign intelligence information "shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand

communications are incidentally acquired support the Fourth Amendment reasonableness of the surveillance.²²⁰ “On these facts, incidentally collected communications of non-targeted U.S. persons do not violate the Fourth Amendment.”²²¹

In conclusion, the Court of Review held that the procedures employed by the government were consistent with the considerations of *In re Sealed Case*.²²² Collectively, they required a showing of particularity, a “meaningful probable cause determination,” a showing of necessity, and a reasonable durational limit.²²³ The risks of error and abuse—which underlay many of the provider’s arguments—were “within acceptable limits and effective minimizations procedures [were] in place.”²²⁴ The court held that, balancing the vital nature of the government’s national security interest and the manner of the intrusion, “the surveillances at issue satisfy the Fourth Amendment’s reasonableness requirement.”²²⁵

V. Conclusion

The Court of Review’s decision in many ways spoke to the issues raised in the debate on the Protect America Act. On the one hand, it recognized the dangers of “indiscriminate executive power” and acknowledged that the “government cannot unilaterally sacrifice constitutional rights on the altar of national security.”²²⁶ Government surveillance for purposes of national security was bound by the Fourth Amendment.²²⁷ On the other hand, the court recognized that the government’s interest in the safety and security of its people was of “utmost significance.”²²⁸ The Court of Review’s role was to

foreign intelligence information or assess its importance.” Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101, 92 Stat. 1783, 1785 (codified at 50 U.S.C. § 1801(h)(2) (2006)).

220. The use of minimization procedures was cited by the Court of Review in its 2002 opinion as an important factor in ensuring the reasonableness of government surveillance under the Fourth Amendment. *In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (citing *Scott v. United States*, 436 U.S. 128, 140–43 (1978)).

221. *In re Directives*, 551 F.3d at 1015.

222. *Id.* at 1016.

223. *Id.*

224. *Id.*

225. *Id.* The Court of Review described in summary form an argument—a “parting shot”—made by the provider for the first time at oral argument regarding “a specific privacy concern that could possibly arise under the directives.” *Id.* at 1015. The court held that, even assuming the provider had not waived this argument, “no issue falling within this description has arisen to date.” *Id.* at 1015. The court directed the government to notify the provider should the issue arise under the directives, but noted that there were safeguards in place that may satisfy the Fourth Amendment’s reasonableness requirement. *Id.* A more detailed discussion of the argument, safeguards, and the court’s holding is provided in the classified version of the court’s opinion. *Id.*

226. *Id.* at 1016.

227. *Id.*

228. *Id.*

balance those considerations.²²⁹ In this case, “where the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions,” the court would not, in its own words, frustrate the government’s efforts to protect national security.²³⁰

The FISA Amendments Act of 2008 that followed the Protect America Act incorporates many of the statutory provisions and procedures that the Court of Review found important to its holding that the government’s surveillance was constitutional.²³¹ In particular, the FISA Amendments Act goes beyond the Protect America Act and imposes, for the first time, the requirement for a judicial finding that a U.S. person outside the United States targeted for surveillance or search is a “foreign power, an agent of a foreign power, or an officer or employee of a foreign power.”²³² This finding is made by the FISC under the FISA Amendments Act; as noted above, this finding was made previously by the Attorney General.²³³ In addition, the FISA Amendments Act expressly bans the “reverse targeting” of U.S. persons²³⁴ and requires FISC approval of the government’s targeting and minimization procedures.²³⁵ Incorporating many of the additional mechanisms the Court of Review relied upon in *In re Directives*, as well as many of the failings critics of the Protect America Act found in that statute, the FISA Amendments Act places on even firmer legal ground the execution of certain Fourth Amendment searches that are permitted by Congress and authorized and implemented by the Executive Branch without prior judicial review.

229. *See id.* (discussing the court’s role in balancing the need to protect individuals from unwarranted intrusions against the nature of the “government’s national security interest and the manner of the intrusion”).

230. *Id.*

231. Amnesty International, among others, has challenged the FISA Amendments Act as unconstitutional. *Amnesty Int’l USA v. McConnell*, 646 F. Supp. 2d 633, 634 (S.D.N.Y. 2009). In August 2009, the district court dismissed this facial challenge for lack of standing, and the appeal is still pending at the time of publication. *Id.* at 658.

232. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 703, 122 Stat. 2436, 2449 (to be codified at 50 U.S.C. § 1881c(b)(3)(B)).

233. *See supra* notes 60, 190-194 and accompanying text.

234. FISA Amendments Act § 702.

235. *Id.*

Programmatic Surveillance and FISA: Of Needles in Haystacks

William C. Banks*

Beginning in 1978, the Foreign Intelligence Surveillance Act¹ (FISA) authorized the means for electronic collection of foreign intelligence that served the nation well for many years. The basic idea was simple. Government may conduct intrusive electronic surveillance of Americans or others lawfully in the United States without traditional probable cause to believe that they had committed a crime if it could demonstrate to a special Article III court that it had a different kind of probable cause: reason to believe that targets of surveillance are acting on behalf of foreign powers.² Over time, FISA was amended several times to extend its procedures to conduct physical searches,³ monitor suspected lone-wolf terrorists,⁴ and accommodate evolving threats.⁵

Over the last decade, critics have argued that the patchwork-like architecture of FISA has become too rigid, complicated, and unforgiving to enable effective intelligence responses to crises.⁶ The computerization of communications that has so enriched our capabilities has also facilitated

* Director, Institute for National Security and Counterterrorism; Board of Advisors Distinguished Professor, Syracuse University College of Law; Professor of Public Administration, Maxwell School of Citizenship & Public Affairs, Syracuse University. The author thanks Spike Bowman, Stephen Dycus, Alexander Joel, Peter Raven-Hansen, Kim Taipale, and the participants in the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology, Feb. 4–6, 2010, for comments on a draft of this article. The author also thanks Andrea Masselli, Syracuse University College of Law, J.D. 2010, for excellent research assistance.

1. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered titles of U.S.C.).

2. *Id.* § 105(a) (codified at 50 U.S.C. § 1805(a)).

3. Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, sec. 807, §§ 301–309, 108 Stat. 3423, 3443–53 (codified as amended at 50 U.S.C. §§ 1821–1829).

4. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001(a), 118 Stat. 3638, 3742 (codified as amended at 50 U.S.C. § 1801(b)(1)(C)).

5. See FISA § 105(b)(2)(B) (requiring an order approving electronic surveillance to direct, at the applicant's request, a communication or other common carrier to assist an applicant in accomplishing the surveillance in a manner to protect its secrecy and minimize interference with the carrier's services); *Id.* § 105(b)(1)(B) (requiring an application to identify the facilities where surveillance will be sought "if known").

6. See, e.g., Richard A. Posner, Op-Ed., *A New Surveillance Act*, WALL ST. J., Feb. 15, 2006, at A16 (arguing that FISA is "dangerously obsolete"); K.A. Taipale & James Jay Carafano, Op-Ed., *Fixing Surveillance*, WASH. TIMES, Jan. 25, 2006, at A15. Judge Posner has claimed that FISA "remains usable for regulating the monitoring of communications of known terrorists, but it is useless for finding out who is a terrorist." Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 252 (2008).

stealth and evasion by those seeking to avoid detection.⁷ Would-be targets of surveillance are communicating in ways that stress or evade the FISA system.⁸ Because of the pervasiveness of U.S. telecom switching technology, collection *inside* the United States is now often the best or only way to acquire even foreign-to-foreign communications that were originally left unregulated by FISA.⁹ Meanwhile, powerful computers and data-mining techniques now permit intelligence officials to select potential surveillance targets from electronic databases of previously unimaginable size.¹⁰ The wholesale quality of this expansive computer collection and data mining is incompatible with the retail scope of the original FISA process.¹¹ Instead of building toward an individual FISA application by developing leads on individuals with some connection to an international terrorist organization, for example, officials now develop algorithms that search thousands or even millions of collected e-mail messages and telephone calls for indications of suspicious activities.¹²

At the same time, more Americans than ever are engaged in international communications, and there is far greater intelligence interest in communications to and from Americans.¹³ Both circumstances increase the likelihood that the government will be intercepting communications of innocent Americans, raising as many questions about the adequacy of FISA safeguards as they do about the adaptability of FISA architecture. This tension forms the context for a series of post-9/11 developments, culminating in the FISA Amendments Act of 2008 (FAA).¹⁴

7. See William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1275–76 (2007) (observing that, in the world of technological surveillance, evasion and logistical difficulties force the government to continually play “catch-up”).

8. *Id.*

9. See David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: Progress to Date and Work Still to Come* (noting that after FISA’s enactment, the need to “conduct surveillance of international communications on wires *inside* the United States” developed, in part because of “the use, location, or accessibility of fiber optic cables”), in *LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM* 217, 226 (Benjamin Wittes, ed., 2009).

10. See, e.g., JAMES BAMFORD, *THE SHADOW FACTORY: THE ULTRA SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA* 12–14 (2008) (describing the vast data-collection capabilities of the NSA).

11. See Josh Meyer & Joseph Menn, *U.S. Spying is Much Wider, Some Suspect*, L.A. TIMES, Dec. 25, 2005, at A1 (investigating concerns that the NSA’s wholesale collection of communication data exceeded FISA and threatened Americans’ privacy).

12. See Shane Harris, *FISA’s Failings*, NAT’L J., Apr. 8, 2006, at 59, 59 (“[T]he NSA’s warrantless eavesdropping program also involves looking for suspicious patterns in a sea of communications.”).

13. See Leslie Cauley, *NSA Has Massive Database of Americans’ Phone Calls*, USA TODAY, May 11, 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm (“[T]he National Security Agency has been secretly collecting the phone call records of tens of millions of Americans . . . [T]he spy agency is using the data to analyze calling patterns in an effort to detect terrorist activity . . .”).

14. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2463 (to be codified in scattered sections of 50 U.S.C.).

The FAA codified a procedure to permit broad, programmatic surveillance focused on patterns of suspicious activities and not on a specific individual or the contents of their communications through changes in FISA that overcame the case-specific orientation of the original statute.¹⁵ As a result, the FAA also codifies, until December 31, 2012, potentially intrusive electronic surveillance unaccompanied by safeguards to protect personal privacy and free expression.¹⁶ The amended FISA also institutionalizes operations that are prone to inaccuracy and chronic overcollection.¹⁷ A 2008 decision by the FISA Court of Review (FISCR),¹⁸ which upheld the government's implementation of the programmatic procedures of earlier but similar temporary legislation¹⁹ by relying on procedures drawn from sources outside FISA, underscores the slapdash development and still-incomplete legal architecture that attends the broad-based programmatic orders.²⁰

From its beginnings, the overarching FISA question has been how to evaluate and weigh the basic values of security and individual liberties when intrusive electronic surveillance is used to collect foreign intelligence. Modern communications and surveillance technologies have so complicated policy discussions, however, that the values debate has drowned in a sea of misapprehension about the means to implement the policies.²¹ Meanwhile, FISA has become so complex that the law further occludes informed policy choices.²² The basic architecture of FISA should be recast.

The Constitution continues to provide a baseline. The Fourth Amendment Warrant Clause applies to electronic surveillance conducted for foreign intelligence purposes within the United States if the surveillance involves U.S. persons who do not have a connection to a foreign power.²³ FISA now

15. See *id.* § 702(a)–(e) (specifying the requirements for acquiring communications data and setting out targeting and minimization protocols).

16. See *id.* § 403 (indicating that the codification is to expire on December 31, 2012).

17. See *infra* notes 105–07 and accompanying text.

18. *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008).

19. Protect America Act of 2007, Pub. L. No. 110-55, §§ 2–3, 121 Stat. 552, 552–55 (to be codified at 50 U.S.C. §§ 1805(a)–(c)).

20. See *In re Directives*, 551 F.3d at 1010 (recognizing the lack of an explicit foreign intelligence exception, but reasoning from the “special needs” cases that an exception to the warrant requirement was appropriate).

21. See Posner, *Privacy, Surveillance, and Law*, *supra* note 6, at 246–47 (discussing modern computer technology and its complication of the values debate shaping lawmaking in the field of electronic surveillance).

22. See Banks, *supra* note 7, at 1214–15 (arguing that the cumulative complexity of FISA has led to the loss of the policy compromise between enabling surveillance and using oversight mechanisms to safeguard individual privacy); Posner, *A New Surveillance Act*, *supra* note 6 (arguing that the “best, and probably the only, way” to clarify the government’s ability to conduct electronic surveillance is to “enact a new statute”).

23. See *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 320–22 (1972) (holding that a warrant is required to conduct domestic surveillance, but limiting that holding to purely domestic threats to national security).

permits such electronic surveillance as the inevitable byproduct of surveillance of unprotected targets, but the Act does little to insulate U.S. persons from the effects of the surveillance. (It is not clear whether the Fourth Amendment Warrant Clause applies to such surveillance when a U.S. person is connected to a foreign power, or when the surveillance of U.S. persons occurs wholly outside the United States. The reasonableness component of the Fourth Amendment does apply in these instances.)²⁴ Historically, our laws have rejected granting discretion for government to undertake intrusive surveillance of individuals without some showing of suspicious activities.²⁵ If the combination of terrorism threats and computerization demands a more nimble capacity to conduct suspicionless electronic surveillance to combat terrorism, the discretion that is necessarily part of that system should be more carefully controlled, either at the point of collection or when the information is maintained or used by the government. Absent such controls, FISA as amended now threatens longstanding Fourth Amendment principles. Apart from its potential constitutional shortcomings, the programmatic surveillance that the FAA permits should be repaired to improve its efficacy. Making the program more efficacious will help make it lawful.

Even before programmatic surveillance was stitched onto FISA, the Act labored under continuing controversies over lowering the wall that separated intelligence from law enforcement investigations²⁶ and the inconsistency of requiring probable cause of foreign agency for targets while permitting surveillance of lone wolves.²⁷ Programmatic surveillance adds considerably to complexity, has already produced implementation problems, and casts doubt on the lawfulness and efficacy of FISA's techniques.

In Part I and Part II of this Article, I will review the FISA model for authorizing surveillance for foreign intelligence purposes and how the combination of evolving technologies and emerging terrorism threats caused FISA to become too unwieldy and inflexible to accommodate the needs for speedy and agile surveillance. In Part III, I will describe how the Bush Administration's Terrorist Surveillance Program (TSP) led to the temporary Protect America Act (PAA), and then to the FAA and the codification of programmatic surveillance. After reviewing a FISCR decision upholding the temporary version of programmatic FISA procedures and taking note of

24. A lower federal court has upheld an exception to the Fourth Amendment Warrant Clause for searches conducted for foreign intelligence purposes outside the United States that involve U.S. persons acting as foreign agents, although in other respects a search still must be reasonable. See *United States v. Bin Laden*, 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000) (adopting a foreign intelligence exception to the warrant requirement for searches targeting foreign powers or their agents conducted abroad). The Supreme Court has not ruled on either set of questions.

25. See *Katz v. United States*, 389 U.S. 347, 361 (1967) (holding that invasion of a constitutionally protected area without a warrant is presumptively unreasonable).

26. Banks, *supra* note 7, at 1241-54.

27. See, e.g., *id.* at 1271-74 (discussing the debate surrounding the adoption of the 2004 Amendment that expanded FISA's reach to unaffiliated persons).

some implementation problems with the FAA in Part IV, in Part V I will suggest some benchmarks for rebuilding FISA from the ground up.

The programmatic features are likely here to stay. For legal and policy reasons, these features should be improved. The thirty-year linchpin of FISA targeting—the location, identity, or both, of the target—should be abandoned where it is not known. Instead, applications for programmatic surveillance under FISA should be based on showing that the proposed electronic surveillance is material to an ongoing investigation of international terrorism or clandestine intelligence activities, that alternative investigative techniques are not capable of collecting the information, and that it is likely that conducting the surveillance will provide the information sought.

A second set of reforms should focus on the retention and dissemination of what is collected. Congress should create a standardized system for authorized use of collected information across the Executive Branch. Building on an authorized-use platform, the Department of Justice and the Office of the Director of National Intelligence should develop guidelines that account specifically for the unique dynamics of protecting personal information about U.S. persons that is collected, even inadvertently, in programmatic collection. In addition, where programmatic surveillance is requested, the FISA Court (FISC) should, before and periodically during implementation, review and approve minimization procedures that are tailored to assess the efficacy and impact on privacy, free expression, and security of the mega-collection and data-mining techniques employed. In the aggregate, a combination of administrative safeguards and judicial and congressional oversight that is more robust than what is now required should be built into the programmatic surveillance portion of FISA.

I. The Original Architecture

Until the FAA, FISA governed the electronic surveillance and physical searches only of persons in the United States and only for the purpose of collecting foreign intelligence.²⁸ (FISA did not apply to surveillance or searches conducted outside the United States or to foreign-to-foreign telephone communications intercepted within the United States.)²⁹ “Probable cause” required that a target of the surveillance be a “foreign power,”³⁰ an “agent of a foreign power,”³¹ or, since 2004, a “lone wolf” terrorism

28. See FISA Amendments Act of 2008, Pub. L. No. 110-261, §§ 701–708, 122 Stat. 2436, 2438–59 (to be codified at 50 U.S.C. §§ 1881–1881g) (relating to “Persons Outside the United States”).

29. See Banks, *supra* note 7, at 1230 (explaining that in 2008 the definition of *electronic surveillance* excluded surveillance taking place abroad).

30. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 105(a)(3)(A), 92 Stat. 1783, 1790 (codified at 50 U.S.C. § 1805(a)(3)(A) (2006)).

31. *Id.*

suspect.³² Applications to the FISC for approval of a search or surveillance had to specify “facilities” where the surveillance would be directed³³ and procedures to “minimize” the acquisition, retention, and dissemination of information not relevant to an investigation.³⁴ A special court, the FISC, which meets in secret, was created to hear requests for orders to conduct the surveillance.³⁵

For a long time the process worked well as a mechanism to regulate surveillance of known intelligence targets.³⁶ The FISA process and its eventual orders have always been limited, however. FISA was concerned with acquisition, not with the uses government might have for what is collected. FISA also assumed that officials know where the target is and what facilities the target will use for his communications.³⁷ Knowing this much enabled the government to demonstrate the required probable cause to believe that the target was an agent of a foreign power or a lone wolf.³⁸ FISA did *not* authorize intelligence collection for the purpose of *identifying* the targets of surveillance, or of collecting aggregate communications traffic and then identifying the surveillance target.³⁹ In other words, FISA envisioned case-specific surveillance, not a generic surveillance operation, and its approval architecture was accordingly geared to specific, narrowly targeted applications.⁴⁰ FISA was also based on the recognition that persons lawfully *in* the United States have constitutional privacy and free expression rights that stand in the way of unfettered government surveillance.⁴¹

Although the volume of FISA applications increased gradually through the 1990s,⁴² after 9/11 the pace of electronic intelligence collection quickened, and Bush Administration officials argued that traditional FISA procedures interfere with necessary “speed and agility.”⁴³ As the pre-9/11

32. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 101(b)(1), 118 Stat. 3638, 3742 (codified as amended at 50 U.S.C. § 1801(b)(1)(C) (2006)) (defining *agent of a foreign power* as “any person other than a United States person, who engages in international terrorism or activities in preparation therefore”).

33. FISA § 105(b)(1)(B).

34. FISA § 101(h); *see also* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, sec. 807, § 301(4), 108 Stat. 3423, 3443–44 (codified at 50 U.S.C. § 1821(4) (2006)) (amending FISA to include a new definition for “minimization procedures”).

35. FISA § 103.

36. *See* Banks, *supra* note 7, at 1233–40 (detailing the operation of FISA between 1978 and the early 1990s).

37. Banks, *supra* note 7, at 1231–32.

38. *Id.* at 1260.

39. *Id.* at 1276.

40. *Id.*

41. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 105(a)(3)(A), 92 Stat. 1783, 1790 (codified at 50 U.S.C. § 1805(a)(3)(A) (2006)).

42. Banks, *supra* note 7, at 1233–34.

43. *Administration Defends NSA Eavesdropping to Congress*, CNN.COM, Dec. 23, 2005, <http://www.cnn.com/2005/POLITICS/12/23/justice.nsa/index.html>.

FISA applications doubled to more than 2,000 a few years later,⁴⁴ the Director of National Intelligence (DNI) complained that more than “200 man hours” are required to prepare an application “for one [phone] number.”⁴⁵ The system was, it seemed, grinding along, but it was carrying a lot of weight.

II. Technological Stresses on FISA

Meanwhile, with the revolution in digital communications, the idea of a geographic border has become an increasingly less viable marker for legal authorities and their limits. Using the Internet, packets of data that constitute messages travel in disparate ways through networks, many of which come through or end up in the United States.⁴⁶ Those packets and countless Skype calls and instant messages originate from the United States in growing numbers, and the sender may be in the United States or abroad.⁴⁷ Likewise, it may or may not be possible to identify the sender or recipient by the e-mail addresses or phone numbers used to communicate.⁴⁸

Nor do we think of our international communications as being in any way less private than our domestic calls. Congress apparently exempted from FISA international surveillance conducted abroad because, when FISA was enacted, electronic communications by Americans did not typically cross offshore or international wires.⁴⁹ Now, of course, we do communicate internationally and our message packets may travel a long distance, even if we are corresponding by e-mail with a friend in the United States who is in the same city.⁵⁰ The location or identity of the communicants is simply not a useful marker in Internet communications. As former CIA Director General Michael Hayden said, “[t]here are no area codes on the World Wide Web.”⁵¹

44. Letter from Brian A. Benczkowski, Principal Deputy Assistant Att’y Gen., U.S. Dep’t of Justice, to Nancy Pelosi, Speaker, U.S. House of Representatives 1 (Apr. 30, 2008), available at <http://www.fas.org/irp/agency/doj/fisa/2007rept.pdf>.

45. Chris Roberts, *Transcript: Debate on the Foreign Intelligence Surveillance Act*, EL PASO TIMES, Aug. 22, 2007, available at http://www.elpasotimes.com/news/ci_6685679.

46. Banks, *supra* note 7, at 1294.

47. See Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. CHI. L. REV. 225, 234–35 (observing that due to “the dominant role of the United States in modern communications technology . . . [c]ommunications service providers in the United States end up playing host to a great deal of traffic sent and received from individuals located abroad”).

48. *Id.* at 35.

49. See *FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 9th (2006) (testimony by Michael V. Hayden, Director, CIA, Office of the Director of National Intelligence), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_senate_hearings&docid=f:43453.pdf (“When [FISA] was passed, almost all local calls were on a wire and almost all long haul communications were in the air.”).

50. *Id.*

51. *Id.* at 7.

Because FISA was written to apply to broadly defined forms of “electronic surveillance”⁵² acquired inside the United States, digital technologies brought the interception of previously unregulated communications inside the FISA scheme.⁵³ In particular, digitization brought e-mail communications within the FISA scheme.⁵⁴ Because of the definition of “electronic surveillance,” even a foreign-to-foreign e-mail message could not be acquired from electronic storage on a server inside the United States except through FISA procedures.⁵⁵ While foreign-to-foreign telephone surveillance was expressly left unregulated by Congress, coverage of e-mail by FISA created an anomalous situation for investigators.

Even an exemption carved out of FISA for foreign-to-foreign e-mail would be problematic because it is often not possible to verify the location of the parties to a communication.⁵⁶ A broader authorization for e-mail surveillance would inevitably include U.S. person senders or recipients and even wholly domestic e-mail. A foreign-to-foreign e-mail exemption would effectively leave in place the requirement of individual FISA applications for overseas targets using e-mail that rely on an ISP in the United States because

52. FISA defines “electronic surveillance” as

(1) the acquisition by an electronic . . . device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic . . . device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States . . . ;

(3) the intentional acquisition by an electronic . . . device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic . . . device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(f), 92 Stat. 1783, 1785 (codified at 50 U.S.C. § 1801(f)(1)–(4)).

53. See Kris, *supra* note 9, at 223 (noting that technological change from communications satellites to undersea fiber-optic cables has caused the scope of FISA to expand).

54. See Rebecca A. Copeland, *War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America*, 35 TEX. TECH. L. REV. 1, 20 (2004) (noting that the USA PATRIOT Act essentially “puts email and internet communication within the purview of clandestine FISA surveillance”).

55. Kerr, *supra* note 47, at 230–32 (reporting that the provision was written to cover microphone bugs and closed-circuit television surveillance, but its original, unchanged terms apply to surveillance of foreign-to-foreign e-mail messages from inside the United States).

56. *Strengthening FISA: Does the Protect America Act Protect Americans’ Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 47 (2007) [hereinafter *Strengthening FISA*] (statement of James A. Baker, Harvard Law School, Former Counsel for the Office of Intelligence Policy and Review, United States Department of Justice).

government could neither ferret out incoming or outgoing U.S. messages in real time nor ignore those messages.⁵⁷

Changing technologies have also turned the traditional sequence of FISA processes on its head. We discovered after 9/11 that investigators could enter transactional data about potential terrorists and come up with a list that included four of the hijackers⁵⁸—a sort of reverse of the typical FISA-supported investigation. Now our intelligence agencies see the potential benefits of data mining⁵⁹—the application of algorithms or other database techniques to reveal hidden characteristics of the data and infer predictive patterns or relationships⁶⁰—as a means of developing the potential suspects that could be targets in the traditional FISA framework. In order to collect the foreign intelligence data, officials claim that they need to access the telecom switches inside the United States so that they can conduct surveillance of e-mails residing on servers in the United States.⁶¹ The mined data would necessarily include data of U.S. persons.⁶²

III. Programmatic Electronic Surveillance

A. *The Terrorist Surveillance Program*

After 9/11, President George W. Bush ordered an expanded program of electronic surveillance by the National Security Agency (NSA) that simply ignored FISA requirements.⁶³ In December 2005, the *New York Times* reported that President Bush secretly authorized the NSA to eavesdrop on Americans and others inside the United States to search for evidence of

57. Kris, *supra* note 9, at 229.

58. Kristen Breitweiser, *Enabling Danger (Part One)*, HUFFINGTON POST, Aug. 20, 2005, http://www.huffingtonpost.com/kristen-breitweiser/enabling-danger-part-one_b_5951.html. Media reports indicated that four of the hijackers had been identified in the summer of 2000 by a data-mining program called Able Danger, run by the Defense Intelligence Agency. *Id.*

59. See TECH. AND PRIVACY ADVISORY COMM., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 45–48 (2004), available at <http://www.cdt.org/security/uusapatriot/20040300tapac.pdf> (recommending privacy protections and recognizing that data mining can “serve many useful purposes in the fight against terrorism and other crimes”). Nearly 200 data-mining programs are in use or are being developed by the government. U.S. GEN. ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 2 (2004), available at <http://www.gao.gov/new.items/d04548.pdf>. This includes fourteen dedicated to analyzing intelligence and detecting terrorists. Jeff Jonas & Jim Harper, CATO Institute, Policy Analysis No. 584, *Effective Counterterrorism and the Limited Role of Predictive Data Mining* 5 (2006), available at http://www.cato.org/pub_display.php?pub_id=6784.

60. K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 6 (2003).

61. See TECH. AND PRIVACY ADVISORY COMM., *supra* note 59, at 27–28 (explaining that the USA PATRIOT covers “addressing and routing” Internet communications).

62. See *id.* at 33–41 (describing the implications of government data mining on U.S. persons).

63. GLEN A. FINE, OFFICE OF THE INSPECTOR GEN. OF THE DEP’T OF JUSTICE ET AL., REPORT NO. 2009-0113-AS, (U) UNCLASSIFIED REPORT ON THE PRESIDENT’S SURVEILLANCE PROGRAM 5–7 (2009), available at <http://www.fas.org/irp/eprint/psp.pdf>.

terrorist activity without obtaining orders from the FISC.⁶⁴ Although the details of what came to be called the Terrorist Surveillance Program (TSP) have not been made public, NSA apparently monitored the telephone and e-mail communications of thousands of persons inside the United States where one end of the communication was outside the United States and where there were reasonable grounds to believe that a party to the international communication was affiliated with al Qaeda or a related organization.⁶⁵

From subsequent accounts and statements by Bush Administration officials it appears that the TSP operated in stages.⁶⁶ With the cooperation of the telecommunications companies, the NSA first engaged in wholesale collection of all the traffic entering the United States at switching stations—so-called vacuum cleaner surveillance.⁶⁷ Second, those transactional data—addressing information, subject lines, and perhaps some message content—were computer mined for indications of terrorist activity.⁶⁸ Third, as patterns or indications of terrorist activity were uncovered, intelligence officials at NSA reviewed the collected data to ferret out potential threats, at the direction of NSA supervisors.⁶⁹ Finally, the targets selected as potential threats were referred to the FBI for further investigation, pursuant to FISA, and the human surveillance ended for the others.⁷⁰

At first the Bush Administration defended the legality of the TSP vigorously, but it was an uphill struggle.⁷¹ In the face of mounting criticism and litigation challenging TSP, the Administration persuaded the FISC to take over supervision of the program,⁷² presumably within the statutory parameters of FISA. When the FISC took over administration of the TSP program in January 2007, Attorney General Alberto Gonzales advised that a FISC judge “issued orders authorizing the Government to target for collection

64. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

65. President George W. Bush, Press Conference on the Post-September 11 Intelligence Gathering Program (Dec. 19, 2005), available at <http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html>; see also U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 5 (2006) [hereinafter DOJ WHITEPAPER] (“The President has acknowledged that . . . he has authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations.”).

66. See FINE, *supra* note 63, at 15–16 (describing the layers of review that the PSP engaged in to target al Qaeda activity).

67. Posner, *Privacy, Surveillance, and Law*, *supra* note 6, at 253.

68. *Id.*

69. *Id.*

70. See FINE, *supra* note 63, at 17 (describing the FBI’s role in the TSP as a recipient of the intelligence ultimately collected).

71. See *id.* at 11–14, 20 (outlining the arguments in favor of the legality of and presidential authority to authorize the TSP).

72. See Eric Lichtblau & David Johnston, *Court to Overturn U.S. Wiretapping in Terror Cases*, N.Y. TIMES, Jan. 18, 2007, at A1 (reporting that the Bush Administration agreed to submit the NSA’s wiretapping program to the supervision of the FISA Court).

international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization.”⁷³ According to the Attorney General, all surveillance that had been occurring under the TSP would now be conducted with the approval of the FISC.⁷⁴

Although the legal basis for fitting TSP inside FISA during this period has not been disclosed, the government must have persuaded at least one FISC judge to treat the international telecom switches as FISA “facilities.”⁷⁵ Because it could reasonably be argued that al Qaeda was using the switches for communications entering and leaving the United States, a few FISC orders gave the government access to nearly all of the international telecom traffic entering and leaving the United States.⁷⁶ The fact that the rest of us were using those switches at the same time was, presumably, dealt with through some version of FISA minimization procedures, where Executive Branch personnel would cull what looked like al Qaeda communications from the mass of data.⁷⁷

B. *The Protect America Act of 2007*

A different FISC judge decided in April 2007 not to continue approval of what had been the TSP under FISC supervision, and apparently determined that at least some of the foreign communications acquired in the United States pursuant to the program are subject to individualized FISA processes.⁷⁸ After a backlog of FISA applications developed, the Bush Administration successfully persuaded Congress to pass statutory authorization for programmatic surveillance outside the case-specific FISA processes.⁷⁹

The Administration emphasized the need to amend FISA to account for changes in technology and thus enable it to conduct surveillance of foreign

73. Letter from Alberto R. Gonzales, Att’y Gen. of the U.S., to Patrick Leahy, Chairman, Comm. on the Judiciary, and Arlen Specter, Ranking Minority Member, Comm. on the Judiciary (Jan. 17, 2007), available at http://www.fas.org/irp.congress/2007_cr/fisa011707.html. He thus implicitly conceded that TSP did fall within the scope of FISA.

74. See FINE, *supra* note 63, at 30 (“Certain activities that were originally authorized as part of the PSP have subsequently been authorized under orders issued by the Foreign Intelligence Surveillance Court (FISC). The activities transitioned in this manner included the . . . ‘Terrorist Surveillance Program.’”).

75. *Id.* at 30–31.

76. FINE, *supra* note 63, at 30.

77. See Kris, *supra* note 9, at 219, 230 (explaining the government is required to adhere to specific “minimization procedures” designed to balance the government’s need to obtain intelligence against the privacy interests of Americans).

78. See *Hearing on the Foreign Intelligence Surveillance Act and Implementation of the Protect America Act Before the S. Comm. on the Judiciary*, 110th Cong. 17 (2007) (statement of J. Michael McConnell, Director of National Intelligence), http://www.dni.gov/testimonies/20070925_testimony.pdf (“[S]ome have advocated for a proposal that would exclude only ‘foreign-to-foreign’ communications from FISA’s scope.”).

79. See FINE, *supra* note 63, at 9–13 (describing key features of the PAA and the scope of its coverage).

digital communications from within the United States.⁸⁰ Yet providing statutory access to U.S. digital telecommunications switches would enable NSA to access e-mail traffic traveling to or from U.S. servers, thus opening up a vast swath of U.S. person communications for government scrutiny.⁸¹

As enacted in August 2007, the Protect America Act determined that the definition of “electronic surveillance” in FISA would not apply to surveillance of a person reasonably believed to be outside the United States.⁸² The PAA also permitted the Director of National Intelligence and the Attorney General to authorize collection of foreign intelligence from within the United States “directed at” persons reasonably believed to be outside the United States, without obtaining an order from the FISC, even if one party to the communication was a U.S. citizen inside the United States.⁸³ Because a FISA “person” may include groups or foreign powers,⁸⁴ surveillance “directed at” al Qaeda permitted warrantless surveillance of the telephones and e-mail accounts of any U.S. person if the government was persuaded that the surveillance was directed at al Qaeda.⁸⁵

The PAA thus made less onerous the determination that the target is known to be abroad. Comparing the PAA to the TSP (as characterized by Attorney General Gonzales), the main differences were that the TSP allowed surveillance of targets inside the United States, and the predicate for collection authority under the PAA was the location of the target, not his status in relation to a foreign power or terrorist organization (as it was under the TSP).⁸⁶

C. *The FISA Amendments Act of 2008*

The PAA expired by its own terms in February 2008 after Congress and the Administration failed to agree on a set of provisions that would grant broad, retroactive immunity to telecommunications firms that participated in the TSP.⁸⁷ The FISA Amendments Act of 2008, enacted in July 2008, conferred the immunity sought by the Administration and the

80. See *id.* at 5–7 (“FISA’s definition of electronic surveillance, prior to the Protect America Act and as passed in 1978, has not kept pace with technology.”).

81. See *id.* (“Thus, technological changes have brought within FISA’s scope communications that the 1978 Congress did not intend to be covered.”).

82. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (to be codified at 50 U.S.C. §§ 1803, 1805a–1805c).

83. *Id.*

84. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(m), 92 Stat. 1783, 1786 (codified at 50 U.S.C. § 1801(m) (2006)).

85. Kris, *supra* note 9, at 32–33.

86. See David Kris, A Guide to the New FISA Bill, Part II, June 25, 2008, available at <http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-ii.html> (noting that the PAA “focuses only on the target’s location (or the government’s reasonable belief about his location) not his status or conduct as a terrorist or agent of a foreign power”).

87. Eric Lichtblau, *Rhetoric: High; Anxiety: Low*, N.Y. TIMES, Mar. 1, 2008, at A11.

telecommunications industry,⁸⁸ and it authorized until December 31, 2012, sweeping and suspicionless programmatic surveillance from inside the United States.⁸⁹

In essence, the FAA codified the PAA—with some additional wrinkles. The core of the new subtitle of FISA retains the broad-based authorization for the Attorney General and DNI to authorize jointly, for a period up to one year, the “targeting” of non-U.S. persons “reasonably believed to be located outside the United States to acquire foreign intelligence information.”⁹⁰ The FISC does not review individualized surveillance applications, and it does not supervise implementation of the program.⁹¹ The FAA does prohibit the government from “intentionally target[ing] any person known at the time of acquisition to be located in the United States.”⁹² However, the government cannot reliably know a target’s location, nor often the target’s identity.⁹³ These uncertainties, combined with the fact that the targeted person may communicate with an innocent U.S. person, mean that the authorized collection may include the international or even domestic communications of U.S. citizens and lawful residents.

Under the FAA, the Attorney General submits procedures to the FISC by which the government will determine that acquisitions conducted under the program meet the program targeting objectives and satisfy traditional FISA minimization procedures.⁹⁴ Although the procedures are classified, we know that they are designed to limit the acquisition, retention, and dissemination of private information acquired during an investigation.⁹⁵ The application to the FISC must also contain a certification and supporting affidavit,⁹⁶ and “targeting procedures” designed to ensure that collection is limited to non-U.S. persons reasonably believed to be outside the United States and to prevent the intentional acquisition of communications where

88. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 703, 122 Stat. 2436, 2441 (to be codified at 50 U.S.C. § 1881a(h)(3)) (“No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance . . .”).

89. Lichtblau, *supra* note 87; *see also* FISA Amendments Act § 403 (indicating that the codification is to expire on December 31, 2012).

90. FISA Amendments Act § 702.

91. *See* Kris, *supra* note 86 (“[T]here is no requirement that anyone—the FISA Court or the NSA—find probable cause that the target is a terrorist or a spy before (or after) commencing surveillance.”).

92. FISA Amendments Act § 702.

93. *See supra* notes 46–51 and accompanying text.

94. FISA Amendments Act § 404. The requirements for minimization in the review of individualized applications for FISA surveillance are codified in 50 U.S.C. §§ 1801(h), 1821(4). Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(h), 92 Stat. 1783, 1785–86 (codified at 50 U.S.C. §§ 1801(h), 1821(4) (2006)). Both sections direct the Attorney General to promulgate detailed minimization procedures. *Id.* The procedures are classified. *Id.*

95. *Id.* § 101. The requirements for minimization are subject to the government’s need to “disseminate foreign intelligence information.” *Id.*

96. FISA Amendments Act § 404.

the sender and all known recipients are known at the time to be located in the United States.⁹⁷ The certification and supporting affidavit must state that the Attorney General has adopted “guidelines” to ensure that statutory procedures have been complied with, that the targeting and minimization procedures and guidelines are consistent with the Fourth Amendment, and that a significant purpose of the collection is to obtain foreign intelligence information.⁹⁸

As with the PAA and the TSP, the FAA does not limit the government to surveillance of particular, known persons reasonably believed to be outside the United States, but instead authorizes so-called “basket warrants” for surveillance and eventual data mining. In addition, non-U.S. person targets do not have to be suspected of being an agent of a foreign power nor, for that matter, do they have to be suspected of terrorism or any national security or other criminal offense, so long as the collection of foreign intelligence is a significant purpose of the surveillance.⁹⁹ Potential targets could include, for example, a non-governmental organization, a media group, or a geographic region. That the targets may be communicating with innocent persons inside the United States is not a barrier to surveillance.¹⁰⁰

For the first time, surveillance intentionally targeting a U.S. citizen reasonably believed to be abroad is subject to FISA procedures.¹⁰¹ As a practical matter, this increased protection for Americans may be illusory. The government may not target a particular U.S. person’s international communications pursuant to its programmatic authorizations, whether the person is in the United States or abroad.¹⁰² Yet officials could authorize broad surveillance, for example, of all international communications of the residents of Detroit on the rationale that they were targeting foreign terrorists who may be communicating with persons in a city with a large Muslim population.

Unlike traditional FISA applications, the government is not required to identify the facilities, telephone lines, e-mail addresses, places, or property where the programmatic surveillance will be directed.¹⁰³ Under the FAA, targeting might be directed at a terrorist organization, a set of telephone numbers or e-mail addresses, or perhaps at an entire ISP or area code.¹⁰⁴

97. *Id.*

98. *Id.*

99. FISA § 101.

100. *See* Kris, *supra* note 86 (positing that the problem was solved, or “dealt with,” via “minimization”).

101. *Compare* FISA Amendments Act § 703(a)(1), *with id.* § 702(a).

102. *See* Kerr, *supra* note 47, at 230 (revealing that FISA, as enacted in 1978, prohibited the government from intentionally targeting the phone calls of “a particular, known United States person” from either outside the United States or within it).

103. FISA Amendments Act § 702.

104. *See, e.g.*, Editorial, *Compromising the Constitution*, N.Y. TIMES, July 8, 2008, at A20 (criticizing the FAA in part because the federal government would be permitted to listen “to all calls

After a FISC judge approves the program features,¹⁰⁵ Executive Branch officials authorize the surveillance and issue directives requesting (or, through an additional court order, compelling) communications carriers to assist.¹⁰⁶ Although details of the implementation of the program authorized by the FAA are not known, a best guess is the government uses a broad vacuum-cleaner-like first stage of collection, focusing on transactional data, where wholesale interception occurs following the development and implementation of filtering criteria. Then NSA engages in a more particularized collection of content after analyzing mined data.¹⁰⁷

Incidental acquisition of the communications of U.S. persons inside the United States inevitably occurs due to the difficulty of ascertaining a target's location and because targets abroad may communicate with innocent U.S. persons.¹⁰⁸ The FAA does nothing to assure U.S. persons whose communications are incidentally acquired that the collected information will not be retained by the government.

Historically, minimization has been conducted during law enforcement investigations to protect against the acquisition of private information unrelated to the purpose of the criminal investigation.¹⁰⁹ The protection of civil liberties through minimization during law enforcement surveillance occurs up front rather than during retention or dissemination in part because electronic surveillance during traditional law enforcement investigations is episodic and short term. Even with traditional FISA electronic surveillance, the authorization is broader and allows for continuous and longer term monitoring, with the understanding that information irrelevant to the

to a particular area code in any other country"); Ryan Singel, *Dems Agree to Expand Domestic Spying, Grant Telecoms Amnesty*, WIREd, June 19, 2008, <http://www.wired.com/threatlevel/2008/06/dems-agree-to-e/> (indicating that under the FAA, "the intelligence community will be able to issue broad orders to U.S. ISPs, phone companies and online communications services like Hotmail and Skype to turn over all communications that are reasonably believed to involve a non-American who is outside the country"); Ryan Singel, *House Grants Telecom Amnesty, Expands Spying Powers*, WIREd, June 20, 2008, <http://www.wired.com/threatlevel/2008/06/house-grants-te/> (indicating that the FAA allows the NSA "to order phone companies, ISPs and online service providers to turn over all communications that have one foreigner as a party to the conversation").

105. FISA Amendments Act § 702. FISC approval of a written certification from the Attorney General and DNI must occur prior to implementation of the authorization for surveillance, unless the same officials determine that time does not permit the prior review, in which case the authorization must be sought as soon as practicable, but not more than seven days after the determination is made. *Id.*

106. *Id.*

107. See Posner, *Privacy, Surveillance, and Law*, *supra* note 6, at 253 (describing the NSA process of "content filtering" and "traffic analysis").

108. *Id.* at 252.

109. See *Berger v. New York*, 388 U.S. 41, 58–59 (1967) (striking down an electronic surveillance statute because it allowed acquisition of "the conversations of any and all persons coming into the area covered by the device . . . indiscriminately and without regard to their connection with the crime under investigation").

investigation will be collected.¹¹⁰ Thus, according to a 2002 opinion of the FISC,¹¹¹ the government conducts FISA minimization after processing (including transcription, translation, and analysis), and the retained foreign intelligence enters an indexed storage system for retrieval.¹¹² In explaining the minimization challenges inherent in foreign intelligence surveillance, the FISC stated in 2002, “[g]iven the targets of FISA surveillance, it will often be the case that intercepted communications will be in code or a foreign language for which there is no contemporaneously available translator, and the activities of foreign agents will involve multiple actors and complex plots.”¹¹³ In addition, unlike the targets of FISA surveillance, Title III targets eventually receive notice that they have been subject to surveillance. They may sue for Fourth Amendment violations, seek to suppress the evidence in a prosecution, or both.¹¹⁴ Traditional FISA minimization protects only nonpublic information concerning U.S. persons who have not consented to acquisition, retention, or dissemination of their personal information,¹¹⁵ and FISA permits the government to retain all information that could be considered foreign intelligence.¹¹⁶

The generic FISA minimization requirements were not modified in the FAA to accommodate the surveillance of individual targets through programmatic surveillance.¹¹⁷ The FAA requires that the Attorney General and the DNI certify that minimization procedures have been or will be submitted for approval to the FISC prior to, or within seven days following, implementation.¹¹⁸ However, the FISC does not review the implementation of minimization procedures or practices for the programmatic surveillance it approves, and FISA permits the government to retain and disseminate information relating to U.S. persons so long as the government determines that it

110. See *In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (“[I]n practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications.”).

111. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611 (FISA Ct. 2002), *abrogated by In re Sealed Case*, 310 F.3d at 717.

112. *Id.* at 617–18; see also *In re Sealed Case* 310 F.3d at 740 (“[I]n practice FISA surveillance devices are normally left on continuously, and the minimization occurs in the process of indexing and logging the pertinent communications.”).

113. *In re Sealed Case*, 310 F.3d at 741.

114. Compare 18 U.S.C. § 2518(9) (2006), with Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 106(f), 92 Stat. 1783, 1794 (codified at 50 U.S.C. § 1806(f)).

115. See FISA § 101(h)(1) (defining minimization procedures to mean “specific procedures . . . designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons”).

116. *In re All Matters*, 218 F. Supp. 2d at 617–18. Early experience with minimization under FISA is reviewed in Helene E. Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs Are Doing Their Jobs*, 12 RUTGERS L.J. 405 (1981).

117. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2439 (to be codified at 50 U.S.C. § 1881a(e)).

118. FISA Amendments Act § 702.

is “foreign intelligence information.”¹¹⁹ By implication, the government may compile databases containing foreign intelligence information from or about U.S. persons, retain the information indefinitely, and then search the databases for information about specific U.S. persons.

Viewing minimization as it evolved from Title III to traditional FISA and to the FAA, the original objective—preventing the collection, retention, or dissemination of private information—has been seriously compromised, or so it seems from the public record. The combination of allowing the government to use the foreign intelligence trump card to hold or disseminate information and the lack of judicial oversight of how private communications are filtered out leaves the minimization mechanism short of meeting its goals for programmatic FISA surveillance. Because FISA minimization is already focused on retention and dissemination and not on acquisition, it should be relatively easy to reform FAA minimization to insert controls on executive discretion and assign a monitoring function to the FISC.

The FISC has described its role in authorizing and reviewing surveillance conducted under the FAA as “narrowly circumscribed.”¹²⁰ The FISC must approve an order for programmatic surveillance if it finds that the government’s certification “contains all the required elements,”¹²¹ that the targeting procedures are “reasonably designed” to target non-U.S. persons,¹²² and that the targeting and minimization procedures are consistent with the FAA and the Fourth Amendment.¹²³ The FISC does not supervise the implementation of the targeting and thus does not review the efficacy of specific surveillance targets.

Long-term congressional authorization for programmatic surveillance marks a stark change in FISA. The FAA permits collection without any showing of individualized suspicion (except for U.S. persons targeted abroad) even where collection of U.S. citizens’ communications is the foreseeable consequence of the program orders.¹²⁴ It may be that individualized FISA applications and their foreign agency or lone-wolf probable-cause determinations are relics of the pre-digital age. Congress and the Executive Branch should confront the realities of digital surveillance and develop approval procedures, minimization safeguards, and judicial and legislative oversight mechanisms to govern the use of data mining and related surveillance techniques to better insure that programmatic surveillance protects our security and our liberties.

119. See FISA § 101(h)(2) (indicating that nonpublicly available information can be disseminated in a manner that identifies a U.S. person without their consent when such person’s identity “is necessary to understand foreign intelligence information or assess its importance”).

120. *In re* Proceedings Required by § 702(i) of the FISA Amendments Act of 2008, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008).

121. FISA Amendments Act § 702.

122. *Id.*

123. *Id.*

124. *Id.*

IV. Implementation of Programmatic Surveillance

A. *The Directives Decision*

On January 15, 2009, the FISCER made public portions of its August 22, 2008, decision, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*.¹²⁵ In *Directives*, the FISCER upheld the constitutionality of directives in pursuit of programmatic surveillance issued to an unnamed telecommunications company pursuant to the temporary Protect America Act.¹²⁶ Because the FAA follows the basic thrust of the PAA, the opinion foreshadows the court's view of the now-codified procedures for programmatic surveillance. The telecom followed a statutory provision and challenged orders compelling it to assist with the acquisition of foreign intelligence where the target was a U.S. person reasonably believed to be outside the United States.¹²⁷ The orders were made following a joint determination by the DNI and the Attorney General that the acquisition satisfied a series of criteria, including minimization procedures.¹²⁸

In its heavily redacted opinion—only the second one publicly issued in its thirty year history—the FISCER held that there is a foreign intelligence exception to the Fourth Amendment warrant requirement, based on the “special needs” doctrine, at least in the “defined context” of cooperation directives to a telecom company.¹²⁹ The exception is available for the programmatic purpose of the surveillance because the acquisition goes “beyond ordinary crime control” and foreign intelligence surveillance about “overseas foreign agents” is “particularly intense.”¹³⁰ Fourth Amendment reasonableness was met in this case through a variety of safeguards found outside the statute. The telecom argued that the collection activities would inevitably lead to incidental collection from nontargeted U.S. persons, but, without further explanation or support, the FISCER characterized the concern as “overblown.”¹³¹ If incidental, said the court, the collections do not violate the Fourth Amendment.¹³²

Relying on the FISCER's own 2002 *In re Sealed Case* decision,¹³³ the telecom argued that the procedural protections provided by the FAA were insufficiently analogous to protections found in the earlier version of FISA, including a particularity requirement, prior judicial review for probable cause

125. *In re Directives to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1017–18 (FISA Ct. Rev. 2008).

126. *Id.* at 1011–12.

127. *Id.* at 1006.

128. *Id.* at 1007.

129. *Id.* at 1010–12.

130. *Id.* at 1011.

131. *Id.* at 1015.

132. *Id.*

133. *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002).

of foreign agency, and proxies for any omitted protections.¹³⁴ Despite the absence of these protections, in its 2008 decision the FISC supported the government's contention that Fourth Amendment reasonableness could be constructed from:

at least five components: targeting procedures, minimization procedures, a procedure to ensure that a significant purpose of a surveillance is to obtain foreign intelligence information, procedures incorporated through Executive Order 12333 § 2.5, and [redacted text] procedures [redacted text] outlined in an affidavit supporting the certifications.¹³⁵

The FISC concluded that the telecom presented no evidence of harm in this instance. According to the court, particularity and prior judicial-review concerns are "defeated by the way in which the statute has been applied."¹³⁶ According to the court, classified procedures approved by the Attorney General, when "combined with the PAA's other protections," and those provided in the Executive Order "are constitutionally sufficient compensation for any encroachments."¹³⁷ The next two subsections evaluate the court's Fourth Amendment analysis.

1. Special Needs.—The special-needs doctrine is a limited exception to the Fourth Amendment warrant requirement. It grew out of searches or surveillance as part of programs that were developed for purposes other than enforcing the criminal laws—searches for drugs in school lockers or immigration checkpoints at our nation's borders, for example.¹³⁸ To invoke the doctrine, the government must show that the primary purpose of its surveillance is something other than law enforcement and that following the warrant and probable cause requirements is impracticable.¹³⁹ If the special needs are accepted, the result is to exempt searches or surveillance authorized by the program from the warrant requirement, leaving reasonableness alone as the more general Fourth Amendment measure.

Following the USA PATRIOT Act amendments to FISA in 2001, the FISC relied in part on the special-needs doctrine to uphold Department of Justice guidelines that permitted criminal investigators to assume lead roles

134. *In re Directives*, 551 F.3d at 1013.

135. *Id.*

136. *Id.*

137. *Id.*

138. *See, e.g., Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (approving warrantless searches that were designed to meet the government's "special needs, beyond the normal need for law enforcement" (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987))).

139. *See Ferguson v. City of Charleston*, 532 U.S. 67, 81–86 (2001) (declaring arrests made pursuant to hospital urine tests unconstitutional because of the policy's law enforcement purpose); *City of Indianapolis v. Edmond*, 531 U.S. 32, 41–47 (2000) (invalidating "drug checkpoints" because the program's primary purpose was to uncover evidence of ordinary criminal wrongdoing); *Griffin*, 483 U.S. at 880 (upholding the supervision of prisoners as a "special need" justifying departure from the warrant process).

in FISA-authorized surveillance so long as “a significant purpose” of the investigation included collecting foreign intelligence.¹⁴⁰ Arguably, the special-needs doctrine should not have been applied in the traditional FISA setting to justify individually targeted electronic surveillance after the “significant purpose” amendment in 2001.¹⁴¹ Although intelligence and law enforcement investigations often overlap in pursuit of national-security or counterterrorism targets, law enforcement officials may exploit the more government-friendly FISA processes and avoid traditional law enforcement rules for securing a warrant when they, and not intelligence investigators, are in charge of an investigation and, from the beginning, are working to build a case for prosecution.¹⁴²

In any case, following the 2002 *In re Sealed Case* FISC decision, the amended statute has been construed to permit the government to engage in “special needs” surveillance when the overriding objective of the surveillance is to gather evidence for prosecution.¹⁴³ The “significant purpose” qualifier applies to programmatic surveillance authorized under the FAA.¹⁴⁴ The use of programmatic surveillance to build a criminal case, such as a large criminal conspiracy, is at least as likely in these instances as in individual FISA applications. Although I continue to doubt the wisdom and lawfulness of the “significant purpose” standard, in the last section of the Article, I propose to accept programmatic surveillance for foreign intelligence as a “special needs” category so long as a series of safeguards are embedded in the system, including a review to assess the importance of the foreign intelligence objective of the surveillance.

2. *Reasonableness.*—The substitutions of individualized FISC review of applications for a traditional warrant and a specialized foreign intelligence related probable cause standard have been construed by nearly every court that has considered their constitutionality as adequate for Fourth Amendment

140. *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002).

141. See Banks, *supra* note 7, at 1282 (asserting that the application of the special-needs doctrine after the “significant purpose” amendment could allow the program to be used even when its sole purpose is the collection of evidence for prosecution without any version of a probable-cause requirement).

142. See *id.* at 1269–70 (noting that FISA should be unavailable if the purpose of the investigation is to prosecute because of FISA’s requirements and the protections of the First, Fourth, and Sixth Amendments).

143. See *Mayfield v. United States*, 504 F. Supp. 2d 1023, 1032 (D. Or. 2007) (holding that “the government can conduct surveillance to gather evidence for use in a criminal case without a traditional warrant, as long as it presents a non-reviewable assertion that it also has a significant interest in the targeted person for foreign intelligence purposes”), *rev’d*, 588 F.3d 1252 (9th Cir. 2009) (declining to address the question of whether the challenged provisions of FISA, as amended by the USA PATRIOT Act, was unconstitutional).

144. *Id.*

purposes.¹⁴⁵ The programmatic orders are so dramatically different from the thirty-year FISA experience, however, that their suspicionless targeting procedures may not be reasonable in Fourth Amendment terms.

In the circumstances of foreign intelligence surveillance designed to counter threats of terrorism and to protect the national security, it is no longer realistic to argue that the Warrant Clause and its traditional law enforcement warrants and the criminal law version of probable cause should apply in the foreign intelligence context, at least where the government demonstrates that the foreign intelligence sought is important to an ongoing counterterrorism investigation and that it is impractical to seek a warrant. As such, the FISCRC holding in *Directives* that there is a foreign intelligence exception to the Warrant Clause is not particularly important. Yet the wooden and pasted-together quality of the court's reasonableness analysis is unfortunate, particularly since reasonableness is the only remaining Fourth Amendment criterion for assessing the programmatic surveillance.

The court purported to make a fact-based decision about reasonableness, as applied to the telecom and the directive it was issued.¹⁴⁶ Ironically, reasonableness was constructed by the court in part from minimization, but we have no idea what the minimization entailed. The facts are opaque due to classification and, whatever they reveal, are based on generic authorization for collection of personal information, on targeting procedures that may significantly overcollect U.S. person information, and are developed solely by the government without opportunity for adversarial testing. The FISCRC must have recognized that it was working with especially limited statutory criteria for reasonableness. As a result, the FISCRC reached outside the FAA to an executive order and an affidavit and relied on the assumed good faith of the implementers in deciding that there were adequate protections for the telecom.¹⁴⁷

As an illustration that challenges to electronic surveillance in the foreign intelligence realm should not excuse a thorough reasonableness review, a panel of the Second Circuit affirmed several convictions in the Africa Embassies bombings prosecutions after a much more fulsome and thoughtful assessment of the Fourth Amendment.¹⁴⁸ While the Second Circuit panel began with similar "totality of the circumstances" and balancing quotes from

145. See *In re Sealed Case*, 310 F.3d at 742 ("[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."). But see *Mayfield*, 504 F. Supp. 2d at 1023.

146. See *In re Sealed Case*, 310 F.3d at 377–79.

147. *In re Directives to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1014–15 (FISA Ct. Rev. 2008). In what the FISCRC calls a "parting shot," the telecom raised what the court called "a specific privacy concern." *Id.* at 1015. The court mentioned it only to task the Executive with notifying the telecom if that concern, whatever it is, arises. We cannot know whether the telecom was drawing attention to the inevitability of overcollection, either in general or specifically in this case. *Id.*

148. *In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157 (2d Cir. 2008).

landmark precedents cited by the FISCER,¹⁴⁹ its analysis carefully probed the factual record. Concerning the telephone surveillance conducted as part of the investigation of the bombings, the court found significant privacy invasions during the year-long surveillance, accompanied by limited efforts at minimization.¹⁵⁰ In balancing the intrusion against the government's need to conduct electronic surveillance, the court took into account: the difficulties of pinpointing surveillance of diffuse organizations like al Qaeda; the problems inherent in sorting through much irrelevant information in pursuit of foreign intelligence; the tendency of organizations such as al Qaeda to communicate in code; and the need to sift through foreign languages in finding relevant intelligence.¹⁵¹ No similar fine-grained analysis accompanied the FISCER *Directives* decision.

The FAA enables the government to overhear Americans' most intimate conversations, for periods up to one year, and there is no judicial gatekeeper of administrative discretion—the agencies decide which communications to monitor. Where targeting and minimization requirements monitored by the FISC help show reasonableness in the traditional FISA setting, programmatic FISA surveillance leaves targeting and minimization so unbounded that the two features do little to assure Fourth Amendment reasonableness. Reasonableness requires a careful evaluation of the government's conduct, and neither the FAA nor the *Directives* opinion contain the necessary review.

One rejoinder to the *Directives* court's scattershot construction of reasonableness is that Congress improved the scheme in enacting the permanent FAA one year later by requiring probable cause of foreign agency for surveillance targeting U.S. persons abroad or intentional targeting of U.S. persons domestically.¹⁵² Still, incidental collection of U.S. person communications inside the United States was not addressed by the FAA, and the *Directives* decision does not assess the reasonableness of such collection.

The FISCER conclusion that “incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful”¹⁵³ faithfully parrots Fourth Amendment doctrine¹⁵⁴ but fails to respond to the unique circumstances of programmatic FISA surveillance. Viewing the public record in the *Directives* case, it is impossible to know to what extent the telecom had shown harmful effects of incidental collections.

149. *Id.* at 172 (quoting *Samson v. California*, 547 U.S. 843, 848 (2006)).

150. *Id.* at 175.

151. *Id.* at 175–76.

152. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 703, 122 Stat. 2436, 2448–51 (to be codified at 50 U.S.C. §§ 1881b–1881c).

153. *In re Directives to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1014 (FISA Ct. Rev. 2008).

154. *Id.* at 1015 (citing, e.g., *United States v. Kahn*, 415 U.S. 143, 157–58 (1974)). In *United States v. Butenko*, 494 F.2d 593, 608 (1974), a review of warrantless surveillance for foreign intelligence purposes found that incidental collection that infringes privacy should be reviewed as part of Fourth Amendment reasonableness.

In any case, the FISC did not acknowledge just how significant an intrusion the “incidental” collection could be.

B. Implementing the FAA

A lawsuit filed by the ACLU challenging the constitutionality of the FAA was dismissed on standing grounds in August 2009.¹⁵⁵ Meanwhile, following a periodic review of the procedures and directives implemented following enactment of the FAA, the Justice Department and DNI reported to the FISC in April 2009 that the NSA had been engaging in significant and systematic overcollection of the domestic e-mail messages of Americans.¹⁵⁶ Though apparently inadvertent, the lapses were headline news and prompted congressional investigations.¹⁵⁷ Unsurprisingly, as the NSA uses telecom switching stations and its satellites to intercept millions of messages, one apparent cause of the overcollection of domestic e-mail messages is the ongoing difficulty of determining the location of the surveillance target.¹⁵⁸

As investigations were launched, some members of Congress disputed the contention that the overcollection was inadvertent.¹⁵⁹ Representative Rush Holt, D-N.J., Chair of the House Select Intelligence Oversight Committee, worried that “the people making policy don’t understand the technicalities.”¹⁶⁰ Intelligence officials told the *New York Times* that the NSA exceeded its statutory authorities in implementing eight to ten separate orders issued by the FISC since enactment of the FAA.¹⁶¹ Because each order could permit collection of hundreds or thousands of phone numbers or e-mail addresses, millions of individual communications could have been intercepted, some portion of which would have been domestic communications by U.S. persons.¹⁶²

155. *Amnesty Int’l USA v. McConnell*, 646 F. Supp. 2d 633, 635 (S.D.N.Y. 2009).

156. Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. TIMES, Apr. 6, 2009, at A1.

157. James Risen & Eric Lichtblau, *Extent of E-mail Surveillance Renews Concerns in Congress*, N.Y. TIMES, June 17, 2009, at A1.

158. *Id.*

159. *Id.*

160. *Id.*

161. *Id.*

162. *Id.*; see also Scott Horton, *Operation Pinwale*, HARPER’S MAG., June 18, 2009, available at <http://harpers.org/archive/2009/06/hbc-90005232> (describing a database code named Pinwale that allegedly contains a large volume of Americans’ e-mail messages collected by the NSA).

V. Benchmarks for Reform

A. *Revising Targeting*

“If the government genuinely cannot determine a person’s location, it makes no sense to use geography as a trigger for FISA’s warrant requirements.”¹⁶³

One problematic feature of the FAA is, notwithstanding all the amendments to FISA over the years, that the legislation *follows* the thirty-year FISA model of focusing on targets and their location for the purposes of authorizing and conditioning surveillance and data collection. From the government’s perspective, the disadvantage of relying on the location of the target as a basis for conducting lawful surveillance was mitigated when the FAA changes provided that the government had only to reasonably believe that the target is abroad.¹⁶⁴ However, one inevitable problem with the relaxed standard is that, given the unreliability of the location identifier, more warrantless surveillance of persons inside the United States will occur.

The technical problems of knowing an individual’s location when an electronic communication is sent or received may also be lessened when implementing FAA surveillance through an expansive interpretation of the FISA definition of “person.” The term is broad enough to include diffuse non-state groups such as al Qaeda.¹⁶⁵ The “reasonably believe” standard presumably may be met because, at any one time, some persons affiliated with al Qaeda may be in the United States and some may be abroad; some may be U.S. persons and some may not.

In place of these workarounds, it is time to replace location of a target as a marker for regulation. Just as our national security interests and threats transcend borders, our personal liberties, including free expression and privacy, are expressed globally. If neither security nor personal freedoms are advanced by adhering to the traditional dividing line that prescribes authorities for warrantless electronic surveillance, it is time to find another approach.

One problem, of course, is that foreigners abroad are consumers of U.S. cyberspace. When corresponding with another foreigner, these persons are unprotected by the Fourth Amendment if they lack other ties with the United

163. Kris, *supra* note 9, at 237.

164. *See id.* at 229 (noting that the amendments, pending at the time, only require the “government’s reasonable belief about [a target’s] location,” as opposed to the more demanding requirement of the target’s “status . . . as a terrorist or agent of a foreign power”).

165. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(m), 92 Stat. 1783, 1786 (codified at 50 U.S.C. § 1801(m) (2006)) (defining “person” as “any individual, including any officer or employee of the Federal government, or any group, entity, association, corporation, or foreign power”).

States.¹⁶⁶ There is no reason to limit our intelligence agencies in surveillance of those communications, and the FAA facilitates that collection. Yet if we unleash surveillance at U.S. switches, our laws and policies have not yet devised a way to prevent them from gaining access to the everyday communications of Americans, the dominant consumers of those switches.

I agree with Orin Kerr that much modern surveillance is “data-focused rather than person-focused.”¹⁶⁷ I also agree with Fred Cate that “[t]he absence of a legal regime governing data mining not only fuels privacy concerns, but also runs the risk of compromising the very objectives that data mining is designed to serve.”¹⁶⁸ Where location, identity, or both of a target are unknown, I, like Kerr, recommend a predicate for surveillance that focuses on the nature of the information sought. Whether the electronic surveillance technique consists of collection followed by data mining or collection accompanied by filtering, and whether the information collected is characterized as “terrorist intelligence information,” as Kerr labels it,¹⁶⁹ or foreign intelligence that bears directly on important national-security or counterterrorism objectives,¹⁷⁰ the government should be permitted to conduct warrantless electronic surveillance if it can demonstrate in advance to the FISC that the information cannot be obtained through a less intrusive means and that it likely will collect what is sought.

Another approach would provide a uniform standard for any collection technique that would require a Fourth Amendment warrant if undertaken for law enforcement purposes in the United States.¹⁷¹ Following the current FAA, FISC approval would be required, subject to a probable cause showing that the surveillance will reveal the information sought, if a U.S. person is targeted for FISA surveillance anywhere, if a target is known to be in the United States, or if officials know in advance that a communication is wholly domestic.¹⁷² All other categories of collection could be authorized by Executive Branch officials. Collection of non-content information, such as addressing information, would be permitted after administrative review to ascertain that the collection is material to an ongoing investigation of international terrorism or in pursuit of clandestine intelligence. Electronic

166. See *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274–75 (1990) (rejecting a Fourth Amendment claim based on the fact that the searched person had “no voluntary attachment to the United States”).

167. Kerr, *supra* note 47, 232–33.

168. Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 437 (2008).

169. Kerr, *supra* note 47, at 238.

170. Judge Posner would define the predicate for programmatic surveillance narrowly. “[T]hreats to national security” would include only “threats involving a potential for mass deaths or catastrophic damage to property or to the economy.” Posner, *Privacy, Surveillance, and Law*, *supra* note 6, at 258.

171. See Kris, *supra* note 9, at 235–36 (suggesting changes to the FAA that would apply to communications between a sender and receivers all located in the United States).

172. *Id.*

surveillance of the contents of communication of other categories of targets could be administratively approved following a showing of probable cause that the collection is material to an ongoing investigation of international terrorism or in pursuit of clandestine intelligence, that the information cannot be obtained through a less intrusive means, and that it is likely that the surveillance technique proposed will collect the information.¹⁷³ These or similar reforms could eliminate the “agent of a foreign power” and “lone wolf” categories altogether.

B. What Happens with the Collected Data?—Minimization and Related Issues

We believe the retention and use by IC organizations of information collected under . . . FISA should be carefully monitored.¹⁷⁴

While simplifying the basic targeting and presurveillance approval requirements will improve the overall FISA scheme, so much would be left to the discretion of unelected officials that FISA collection reforms should also focus on postcollection controls. The quotation above from the Inspectors General of DOD, DOJ, CIA, NSA, and ODNI is taken from the conclusions of their report on Bush Administration surveillance activities.¹⁷⁵ Following their lead, minimization should be enhanced for programmatic surveillance to make less likely the misuse of the massive collection of personal information about U.S. persons. Whether or not Fourth Amendment jurisprudence recognizes the collected information as part of our reasonable expectation of privacy,¹⁷⁶ Congress should impose limits on the retention, use, and dissemination of the information collected through FISA programmatic orders or directives.

Every FAA decision bearing on specific intelligence targets is made by Executive Branch officials and is not subject to review by the FISC or another judge.¹⁷⁷ Prior identification of targets to a judge protects innocent third parties from being swept up in the surveillance and enforces the

173. Kerr, *supra* note 47, at 238–39.

174. FINE, *supra* note 63, at 38.

175. *Id.* at 3.

176. See *Warshak v. United States*, 490 F.3d 455, 473–76 (6th Cir. 2007) (finding that individuals have a “reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP” and thus that the government must provide notice and an opportunity to be heard before compelling the ISP to turn over the e-mails to the government), *vacated*, 532 F.3d 521 (6th Cir. 2008) (en banc); see also Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 82–83 (2005) (advocating due process protections in data mining).

177. The FISA Court only reviews targeting and minimization procedures to ensure that they meet the statutory requirements and the Fourth Amendment, and the court only reviews certifications as a matter of form, to ensure that they “contain[] all the required elements.” Kris, *supra* note 86, at 230 (citing FISA Amendments Act, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2444 (to be codified at 50 U.S.C. § 1881a(i)(3)(A)–(B))).

hallmark predicate for government surveillance—individualized suspicion.¹⁷⁸ The breadth of FAA orders and determinations permits vacuum-cleaner-like collection from telecom switches, for example.¹⁷⁹ Once collected, executive officials cull through the data in pursuit of suspicious indicators that merit further investigation.¹⁸⁰ False positives are one inevitable result. Another is the potential for abuses of stored data.¹⁸¹

How do officials determine to look more closely at individualized pieces of the traffic? Apparently NSA uses algorithms that purport to identify terrorist suspects out of the vacuumed mass of data.¹⁸² How exactly could such a data-driven process sort the innocuous call to me from my Muslim friend abroad from one that is worthy of further investigation? Is the limited, follow-on surveillance performed by humans then a minimal intrusion that we should be prepared to accept if we are assured that the brief surveillance will end and a traditional FISA application would follow if further electronic surveillance is deemed worthwhile?¹⁸³

Under traditional, individualized FISA processes, “specific procedures” for minimization must be promulgated by the Attorney General and filed with the FISC for every individual target, “to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.”¹⁸⁴ The case-specific procedures are classified.¹⁸⁵ In these cases, the minimization itself is supervised by the FISC during the course of surveillance,¹⁸⁶ and the court may modify the procedures and order that the

178. See, e.g., Cate, *supra* note 168, at 480, 487 (arguing that prior judicial authorization in data mining would help better balance security with privacy concerns).

179. See Mark Williams, *The Total Information Awareness Project Lives On*, TECH. REV., Apr. 26, 2006, available at <http://www.technologyreview.com/communications/16741> (explaining that when the NSA practices automated data mining, FISA requirements are inapplicable because it is not a search of a specific individual).

180. Cate, *supra* note 168, at 473–74.

181. *Id.* at 471–80.

182. See Williams, *supra* note 179 (stating that the NSA uses electronic analysis and content filtering to apply “highly sophisticated search algorithms and powerful statistical methods . . . [to] search for particular words or language combinations that may indicate terrorist communications”).

183. See K. A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance*, 8 N.Y.U. REV. L. & SECURITY, NO. VII SUPPLEMENTAL BULL. ON L. & SECURITY 3, 5–6 (2006) (so advocating).

184. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 101(h)(1), 92 Stat. 1783, 1785 (codified at 50 U.S.C. § 1801(h)(1) (2006)). The procedures are also sent to the Intelligence Committees in Congress. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702(f)(2)(A), 122 Stat. 2436, 2439 (to be codified at 50 U.S.C. § 1881a(1)(1)(B)).

185. FISA § 106(f).

186. *Id.* § 105(d)(3); Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 304(c)(3), 108 Stat. 3423, 3448 (codified at 50 U.S.C. § 1824(d)(3) (2006)).

modified procedures be followed if it finds that the proposed procedures do not satisfy the FISA definition.¹⁸⁷

By focusing on what the collected information may be used for, FISA and the FISC, until the FAA, provided a useful, albeit opaque, mechanism to ensure the accountability of the collection scheme. To be sure, the government could use and disseminate information about a person who was not the target of the approved surveillance, but whose information was collected inadvertently.¹⁸⁸ In addition, the “consistent with” clause provides a hedge for the government to disclose to law enforcement officials or, presumably, to anyone else foreign intelligence information.¹⁸⁹ Indeed, in discussing the retention stage of minimization, the publicly released 2002 FISC opinion quotes the following standard from the *Justice Department Standard Minimization Procedures for U.S. Person Agent of a Foreign Power*: “communications of or concerning United States persons *that could not be* foreign intelligence information or are not evidence of a crime . . . may not be logged or summarized.”¹⁹⁰ Because minimization “is required only if the information ‘*could not be*’ foreign intelligence,”¹⁹¹ the standard is already extremely friendly to the government.

By its nature, the FAA shifts nearly all the burden of civil liberties protection to postcollection minimization, and there is no publicly known mechanism for tailoring minimization to these new conditions. Executive Branch personnel select which communications are retained and, thus, logged and indexed in some way for ease of retrieval, all without judicial supervision.¹⁹² Relying on the default requirements, by following FAA minimization procedures the government could compile databases of collected information, maintain them, and search them later for information about U.S. persons.¹⁹³

Minimization requirements should be reviewed alongside the predictive abilities of the data-mining methods employed in programmatic

187. FISA § 105(a)(5); Intelligence Authorization Act § 304(a)(5).

188. See *supra* notes 114–17 and accompanying text.

189. See *supra* note 184 and accompanying text.

190. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 618 (FISA Ct. 2002), *abrogated by In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

191. *Id.*

192. It is, of course, also true that the failure of the government to log or index a communication that made that record practically inaccessible when FISA was enacted would not stand in way of retrieval of the record today if officials employed their search software. See DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS 9-22 to -24 (2007) (describing “tensions” between retention and discovery in criminal cases, where useable files are disclosed to the defendant in compliance with *Brady*, including non-pertinent audio files that should have been destroyed or rendered useless following minimization). In other words, even information minimized following traditional FISA practices might still be accessible to the government. *Id.*

193. See *supra* notes 115–17 and accompanying text.

surveillance.¹⁹⁴ In 2008, a committee of the National Research Council found that “automated identification of terrorists through data mining is neither feasible as an objective nor desirable as a goal of technology development efforts.”¹⁹⁵ Apart from the serious privacy intrusions that are an incident of data mining, the committee found that the questionable quality of the data in countering terrorism (in countering terrorism, much of the information collected is unreliable or has unclear meaning),¹⁹⁶ its propensity to lead to false positives, the vulnerability of data mining to countermeasures, and the paucity of scientific evidence supporting data mining argue that, at most, the techniques should be used as a “preliminary screening method for identifying individuals who merit additional follow-up investigation.”¹⁹⁷ Employed only as a “preliminary screening method,”¹⁹⁸ “any information-based counterterrorism program of the U.S. government should be subjected to robust, independent oversight.”¹⁹⁹ For programmatic surveillance pursuant to FISA, their recommendation translates into rigorous minimization focused on retention and dissemination, supervised by the FISC.

The National Research Council acknowledged that traditional minimization “has been rendered largely irrelevant in recent years as technology and applications have evolved so that vast streams of data are recorded and stored, rather than just limited, relevant elements. . . . [E]ven irrelevant data are routinely retained by the government indefinitely.”²⁰⁰ The Council recommends that “[w]henver practicable” personal identifying information should be “removed, encrypted, or otherwise obscured”²⁰¹ before retention or dissemination.

Whether or not required by the Fourth Amendment, minimization that protects against undue retention and dissemination would serve the particularity values that have long been central to Fourth Amendment

194. Daniel J. Solove, *Data Mining and the Security–Liberty Debate*, 75 U. CHI. L. REV. 343, 352–53 (2008).

195. COMM. ON TECHNICAL AND PRIVACY DIMENSIONS OF INFO. FOR TERRORISM PREVENTION AND OTHER NAT’L GOALS ET AL., NAT’L RESEARCH COUNCIL OF THE NAT’L ACADEMIES, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT 3–4 (2008) [hereinafter PROTECTING INDIVIDUAL PRIVACY], available at http://epic.org/misc/nrc_rept_100708.pdf.

196. Cate, *supra* note 168, at 469–70.

197. PROTECTING INDIVIDUAL PRIVACY, *supra* note 195, at 4. The committee offered a detailed framework for prospective development of data-mining programs to combat terrorism. *Id.* at 44–66. *But see* *Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 14 (2007) (testimony by Kim Taipale, Founder and Executive Director, Center for Advanced Studies in Science and Technology Policy), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_senate_hearings&docid=f:33226.pdf (arguing that data mining for counterterrorism is a useful investigative tool that may be tailored to meet government needs and protect privacy).

198. PROTECTING INDIVIDUAL PRIVACY, *supra* note 195, at 4.

199. *Id.* at 5.

200. *Id.* at 55.

201. *Id.*

reasonableness. Since 1976, the Supreme Court has held that there is no reasonable expectation of privacy in data held by a third party.²⁰² Courts have reasoned that, by transferring the information to a third party, such as a bank, phone company, or ISP, the consumer has no reasonable expectation of privacy that prevents the company from sharing the information with the government.²⁰³ The evolving third-party-records doctrine has, in turn, provided the legal basis for a variety of law enforcement and national security-related data-collection schemes by the government, including collection authorized by FISA.²⁰⁴

Because data mining and its techniques are employed after collection, the Fourth Amendment may not control what government does to use or store the collected information.²⁰⁵ Although there are signs that some courts are beginning to question the efficacy of the third-party doctrine in the context of data mining for national-security and counterterrorism purposes,²⁰⁶ a reversal of the Supreme Court rule is unlikely anytime soon.²⁰⁷ Nor would a judicial reversal respond to the shortcomings in regulating data mining for foreign intelligence purposes.²⁰⁸ Instead, Congress and investigating agencies should adopt controls on the use of data mining for foreign intelligence purposes.

During the pre-enactment hearings on FISA more than thirty years ago, Congress recognized that there are “a number of means and techniques which the minimization procedures may require to achieve the purpose set out in the definition.”²⁰⁹ The FISA practice of retaining foreign intelligence has relied on selective logging and indexing of information.²¹⁰ The FISC, in its 2002 *In re All Matters* opinion, closely examined the retention stage, and

202. See *United States v. Miller*, 425 U.S. 435, 442 (1976) (holding a bank customer had no expectation of privacy in checks and deposit slips held by a bank); see also *Smith v. Maryland*, 442 U.S. 735, 742 (1979) (holding there is no expectation of privacy when a pen register is installed on phone company property at the company’s office because people do not reasonably believe there is an expectation of privacy when they “convey” a dialed phone number to the phone company).

203. See *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 742 (both reasoning that the expectation of privacy vanishes when a person voluntarily submits data to a third party).

204. See *Cate*, *supra* note 168, at 454–60 (setting out the Court’s decisions in *Miller* and *Smith* and applying that line of cases today).

205. Solove, *supra* note 194, at 356–57 (finding that the third-party doctrine severely limits Fourth Amendment protections where the government mines data voluntarily given to companies by their customers).

206. Cf. *Warshak v. United States*, 490 F.3d 455, 473, 482 (6th Cir. 2007) (finding Fourth Amendment protection against the government’s warrantless subpoena of e-mails transmitted through a commercial ISP where the fact that it was not the ISP’s normal practice to review e-mails supported users’ reasonable expectation of privacy), *vacated*, 532 F.3d 521 (6th Cir. 2008).

207. *Cate*, *supra* note 168, at 460.

208. *Id.*

209. H.R. REP. NO. 95-1283, pt. 1, at 56 (1978).

210. See *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 618 (FISA Ct. 2002) (outlining the principal steps in the minimization process), *abrogated by In re Sealed Case*, 310 F.3d 717, 736 (FISA Ct. Rev. 2002).

concluded that the critical determination is when “a reviewing official, usually an FBI case agent, makes an informed judgment as to whether the information seized is or might be foreign intelligence information related to clandestine intelligence activities or international terrorism.”²¹¹ If the case agent decides that there is no foreign intelligence information in what is being reviewed, minimization would leave the recorded information off the indexing table: “if recorded[,] the information would not be indexed, and thus become non-retrievable[;] if in hard copy[,] from facsimile intercept or computer print-out[,] it should be discarded[;] if on re-recordable media[,] it could be erased[;] or if too bulky or too sensitive, it might be destroyed.”²¹² Over time, criminal appeals where FISA surveillance was alleged to have been conducted unlawfully revealed that minimized information may nonetheless have been recorded and not destroyed and may remain in some electronic format available for retrieval.²¹³ In programmatic surveillance, NSA personnel likely substitute for the FBI case agent.²¹⁴ The magnitude of the minimization corpus has changed so much that guidelines for ferreting out material to be minimized and for administrative review of retention decisions should be promulgated.

In a September 2007 letter to the House Intelligence Committee, the Civil Liberties Protection Officer for the ODNI explained that minimization procedures then in place at NSA, while not identical to those used for the PAA or FAA, “provide[d] general guidance for the types of processes and requirements involved with minimization.”²¹⁵ Summarizing a declassified version of United States Signals Intelligence Directive 18 (USSID 18), the letter notes that U.S. person communications “may generally only be retained in raw form for a maximum of five years, unless there is a written finding that retention for a longer period is necessary to respond to a foreign intelligence requirement;”²¹⁶ identities of U.S. persons “are generally redacted . . . and replaced with generic terms”;²¹⁷ and U.S. person identities may be released if “necessary to understand foreign intelligence information or assess its importance.”²¹⁸ The letter emphasizes that, in addition to the ODNI

211. *Id.*

212. *Id.*

213. KRIS & WILSON, *supra* note 192, at 9–23.

214. See OFFICE OF DIR. OF NAT’L INTELLIGENCE, ELECTRONIC FRONTIER FOUNDATION FINAL RESPONSE (2007), available at http://www.dni.gov/electronic_reading_room/EFFR%20-%20FOIA.pdf (describing the policy by which the NSA should hand off information to the FBI as part of the minimization procedure).

215. Letter from Alexander W. Joel, Civil Liberties Prot. Officer, Office of the Dir. of Nat’l Intelligence, to Silvestre Reyes & Peter Hoekstra, Representatives, U.S. House of Representatives 6 (Sept. 17, 2007), available at <http://www.fas.org/irp/news/2007/09/joel091707.pdf>.

216. *Id.*

217. *Id.*

218. *Id.*

office, internal oversight of minimization is provided by the National Security Division at DOJ and the Office of General Counsel at ODNI.²¹⁹

In its PAA minimization procedures, discussed by NSA in answering questions from the Intelligence Committees and released following a FOIA request, NSA acknowledged that minimization is “not an exact science,” and yet “analysts over time develop an excellent working knowledge of their targets,” thus making mistakes in collecting foreign intelligence less likely.²²⁰ Reading between the redactions in the declassified answers, it is impossible to obtain a clear picture of minimization practice. NSA does object to codifying minimization procedures “because it can be difficult to change a statute if the procedures need to be changed in order to meet operational needs,” and it notes that NSA “has established extensive compliance mechanisms” to meet PAA requirements, all of which are subject to oversight and review by the NSA SIGINT Directorate Office of Oversight and Compliance, the Office of Inspector General, and the Office of General Counsel, in addition to the ODNI and DOJ.²²¹ While the limited transparency afforded by the ODNI letter and NSA procedures and responses to the Intelligence Committees’ questions promises continuing oversight, these documents do not provide substantive administrative safeguards, much less legislative standards, which would more effectively protect civil liberties following programmatic surveillance.

The most facile means for minimization prior to dissemination pursuant to FISA has been simply to redact U.S. person names and identifiers.²²² In the few settings prior to the FAA where the Attorney General could authorize surveillance without advance FISC approval, there had to be “no substantial likelihood” that the acquisition would reach “the contents of any communication to which a United States person is a party.”²²³ Because Congress recognized that U.S. person-communications collection could nonetheless occur in those situations, minimization required that none of the contents of such a communication could be disseminated “for any purpose or retained for longer than 72 hours” without a court order or an Attorney General determination that the information “indicates a threat of death or serious bodily harm to any person.”²²⁴ Although these steps were contemplated for surveillance undertaken without *any* prior FISC involvement, the limited role that the court plays in approving programmatic surveillance suggests that requiring a

219. *Id.* at 7–8.

220. NSA’s Minimization Procedures, in FOIA REQUEST BY ELECTRONIC FRONTIER FOUNDATION 000301 (Dec. 10, 2007), available at http://www.dni.gov/electronic_reading_room/EFFR%20-%20FOIA.pdf.

221. *Id.* at 000301, 000304.

222. KRIS & WILSON, *supra* note 192, at 9–27; cf. 50 U.S.C. § 1801(h)(2) (2006) (defining “minimization procedures” as those procedures protecting U.S. person identities).

223. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 102(a)(1)(B), 92 Stat. 1783, 1787 (codified at 50 U.S.C. § 1802(a)(1)(B) (2006)).

224. FISA § 101.

court order for dissemination of information about U.S. persons within days of collection through programmatic surveillance may serve the minimization objectives.

In its third report on improving information sharing,²²⁵ a Markle Foundation Task Force recommended responding to the problems of sharing too much or too little information with a government-wide authorized-use standard that “would improve the access, sharing, use, and protection of relevant information legally in the government’s possession while protecting privacy and civil liberties.”²²⁶ In addition to recommending the use of anonymization technology to enable information analysis without disclosure of personal identifying information, the Task Force recognized the need to balance potentially competing goals to account for the sensitivities of U.S. persons, while permitting information sharing to occur in a timely fashion.²²⁷ For information collected that is not about U.S. persons or is not personally identifiable, authorized use could be automatically generated by the digitized system.²²⁸

For such personal information about U.S. persons as is included in information proposed for use or dissemination, the requester would be required to “articulate a more specific authorized use to access that information . . . to meet a higher standard of care and need.”²²⁹ In other words, permission to use the information would be based on the nature and timing of the threat or mission at issue in an investigation. The authorized-use system would be set up so that “the more sensitive the information, the higher the required authorized use, the stricter the audit, and potentially, the greater the need for an official to consider approval for deanonymization.”²³⁰ Under authorized use, auditable records would be maintained for each dissemination, and audits and other forms of monitoring would be utilized to ensure enforcement of authorized use.²³¹

New legislation would prescribe the framework for an authorized-use system, and the Executive Branch would develop agency-specific guidelines or regulations to implement authorized use subject to the agency requirements and to specific legal authorities that apply to the agency’s processes.²³² The process for creating the guidelines or regulations should be as transparent as possible and it should include privacy and civil liberties officers from

225. MARKLE FOUND., MOBILIZING INFORMATION TO PREVENT TERRORISM: ACCELERATING DEVELOPMENT OF A TRUSTED INFORMATION SHARING ENVIRONMENT (2006).

226. *Id.* at 33.

227. *Id.* at 35–36.

228. *Id.* at 35.

229. *Id.*

230. *Id.* at 36.

231. *Id.* at 40. The Task Force also proposed that authorized use include a safe-harbor mechanism that would prohibit punitive action against any user of the system that used collected information following authorized-use guidelines. *Id.* at 40–41.

232. *Id.* at 34–35, 39.

the agencies, review by the Privacy and Civil Liberties Oversight Board, and then final approval by the President.²³³ For programmatic FISA surveillance, the guidelines should formalize standards of care and need for the retention and use of U.S. person information inadvertently collected, and they should require FISC approval of the guidelines and of dissemination decisions where personally identifiable information about individual U.S. persons would be transferred. Anonymization of U.S. person information should be required wherever possible, consistent with lawful surveillance objectives. The guidelines should also specify audit procedures, and the procedures and audit reports should be reported to Congress.

VI. Conclusion

When I first became a student of FISA, more than twenty years ago, I struggled to understand when a friend who worked inside the FISA process told me that we should worry less about what is collected and how and more about how what is collected is used. Eventually I learned about the importance of the now-lowered wall that separated foreign intelligence from law enforcement and about how minimization could protect private information.

Meanwhile the digital revolution and our data-driven society resulted in private industry having access to personal identifying information about most Americans. The constitutional and statutory law grew up around the premise that our voluntary sharing of that personal information with our credit card companies, ISPs, and banks eliminated any reasonable expectation of privacy in that information. When the government more prominently and aggressively began collecting and then mining that stream of data, especially after September 11, only a few limits were set on its use. Yet, when the TSP was exposed based on the same techniques, there was widespread condemnation of the Bush Administration. Why?

Part of the reason is that Americans did not know that the government could be listening in on or viewing their international telecommunications traffic, incoming and outgoing, and we feared that our conversations and e-mails were being monitored by someone at NSA. Once we learned more about the program, we also feared that officials were continuing to monitor our communications without probable cause and without the approval of any judge.

As we learned more about TSP and its follow-on iterations, as authorized by the FISC and then Congress, it became clear that the more significant privacy intrusion occurs not at the initial stage of flagging our calls or e-mails, but at the point when someone, looking at aggregate data for patterns or suspicious activity, decides to personally review an individual's communications. In other words, we should be worried more about what the data is used for, not so much that it is collected.

233. *Id.* at 39.

Although information sharing has been a mantra in recent years, and curtailing the uses of collected data cuts against sharing, important reasons exist for imposing controls in the newest FISA program. Data mining is more than the “automation of traditional investigative skills.”²³⁴ The “automation” may have a greater impact on personal privacy because the mass of data mined will generate more false positives than traditional police work, and, absent controls, the data may be preserved indefinitely for any use, including human review. To defend data mining by arguing, as Judge Richard Posner has, that “[c]omputer searches do not invade privacy because search programs are not sentient beings”²³⁵ is to ignore what happens to the data after it is mined.

Judge Posner concedes that programmatic surveillance produces many false positives But . . . the cost of false positives must be balanced against that of false negatives. . . . The intelligence services have no alternative to casting a wide net with a fine mesh if they are to have reasonable prospects of obtaining the clues that will enable future terrorist attacks on the United States to be prevented.²³⁶

If we accept the utility and inevitability of programmatic collection, it does not undermine collection to insist on targeting criteria that focus on the nature of the information sought and fulsome protections against retaining and disseminating collected personal information.

234. Taipale & Carafano, *supra* note 6, at 21.

235. Posner, *Privacy, Surveillance, and Law*, *supra* note 6, at 254.

236. *Id.* at 252–53.

The Modest Role of the Warrant Clause in National Security Investigations

Orin S. Kerr*

I. Introduction

The Warrant Clause of the Fourth Amendment states that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”¹ In criminal investigations, this clause plays a significant role. As the Supreme Court has emphasized, “it is a cardinal principle that ‘searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.’”² In the setting of national security law, however, the opposite is true. The Warrant Clause plays a role,³ but only a modest one. The Warrant Clause can inspire legislative action, or it can give a thumbs up or down to an existing legislative scheme. But the Warrant Clause does not play the significant role in the national security investigations that it plays in criminal investigations.

Why is the Warrant Clause of the Fourth Amendment so modest in national security investigations? One plausible reason is that national security investigations raise significant questions of presidential power under Article II.⁴ Courts may be hesitant to use the heavy hand of the Warrant Clause when investigations involve presidential prerogatives. Or perhaps the Warrant Clause is narrow because Congress has imposed statutory warrant procedures that limit opportunities for constitutional challenge.⁵ Perhaps. But I think there is another reason and one that is more conceptually interesting from a perspective of Fourth Amendment law. This Article will develop that argument. It argues that the Warrant Clause has been and will remain narrow because the extension of the Warrant Clause into national

* Professor of Law, George Washington University Law School. The author thanks Bobby Chesney for the invitation to participate in the Symposium.

1. U.S. CONST. amend. IV.

2. *Mincey v. Arizona*, 437 U.S. 385, 390 (1978) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). Of course, “specifically established and well-delineated” does not necessarily mean narrow. Nonetheless, warrants play an important role in the criminal law setting.

3. *See, e.g., United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 321 (1972) (imposing a warrant requirement for domestic national security investigations).

4. U.S. CONST. art. II.

5. *See, e.g., 50 U.S.C. § 1823(a)* (2006) (imposing a statutory warrant requirement for physical searches in national security investigations).

security law has come at a cost of forcing courts to pose a question that judges know they cannot answer.

The dynamic goes back to a series of cases in the late 1960s and early 1970s when the Supreme Court dramatically expanded the scope of the Warrant Clause.⁶ The Court reframed the Warrant Clause as a handmaiden of reasonableness: warrants are required only when a warrant requirement would be reasonable, and the warrants that are required are whatever warrants would be reasonable.⁷ This double-barreled reasonableness test gave the Supreme Court the flexibility to insert the Warrant Clause almost anywhere, including the setting of national security investigations. But it came at a cost. The test created to give courts flexibility forces judges to ask a question they are poorly equipped to answer. Faced with uncertainty, most judges will remain cautious. As a result, the Warrant Clause will apply broadly in theory but work modestly in practice.

Courts are poorly equipped to answer when a warrant regime would be reasonable in the national security setting for four major reasons. The first is what I will call the "chicken-and-egg problem." Courts do not know what kind of warrant they must imagine operating because the kind of warrant is itself left open by existing law. Second, the Judiciary cannot know whether the elected branches would set up courts with expert judges or with jurisdiction to issue those warrants, making it difficult for them to assess how such a warrant requirement would work. Third, courts cannot know the technology of surveillance that will apply or whether diplomatic agreements will harmonize the different legal regimes, making it hard to know how warrants would be executed. And fourth, uncertainty as to the law of when national security investigations trigger the Fourth Amendment at all leaves courts uncertain as to what set of facts they will be balancing.

Faced with these uncertainties, courts have and generally will construe the Warrant Clause quite narrowly in national security investigations.⁸ The Warrant Clause can spark action, leaving the details up to Congress. The Clause can also be used to ratify or reject a specific legislative scheme. But it cannot play the same strong role in national security cases that it has traditionally played in criminal investigations. In the national security setting, the Warrant Clause must remain modest.

II. The Surprisingly Flexible Warrant Standard

To understand the cautious role of the Warrant Clause in national security cases, a brief history of the warrant standard is necessary. The text of the Fourth Amendment suggests that the standard for obtaining warrants is

6. See *infra* Part II.

7. See *infra* Part II.

8. See *infra* Part III.

immutable and that the warrant requirement is fixed.⁹ This textual clarity masks a surprisingly amorphous standard, however. The historical development of the warrant standard shows that the Supreme Court has repeatedly changed the warrant standard, both in terms of when warrants are required and what the government must show to obtain a warrant. In expanding the Warrant Clause over time, the Court has applied a surprisingly malleable standard.

A. Arrest Warrants and Search Warrants Before 1967

There are two basic kinds of warrants: arrest warrants and search warrants. The purpose of a search warrant is to authorize a search of a place and the seizure of property found there;¹⁰ the purpose of an arrest warrant is to authorize the arrest of a person.¹¹ Throughout much of our constitutional history, arrest warrants rather than search warrants played the primary role.¹² When the government charged a minor offense by information rather than indictment, the government would file an information but then need a warrant to authorize the suspect's arrest.¹³ In 1877, Justice Bradley explained that an arrest warrant must establish "probable cause of belief or suspicion of the party's guilt."¹⁴ The power to make an arrest then provided powers to make searches incident to arrest.¹⁵

9. U.S. CONST. amend. IV. See generally Wayne R. LaFare, *Administrative Searches and the Fourth Amendment: The Camara and See Cases*, 1967 SUP. CT. REV. 1, 12–13 ("To say that the probable cause required by the Fourth Amendment is not a fixed test, but instead involves a sort of calculus incorporating all the surrounding circumstances of the intended search, constitutes a major departure from existing constitutional doctrine.")

10. A search warrant is "[a] judge's written order authorizing a law-enforcement officer to conduct a search of a specified place and to seize evidence." BLACK'S LAW DICTIONARY 1379 (8th ed. 2004). See generally FED. R. CRIM. P. 41(d)–(e) (explaining that once the issuing magistrate or judge is satisfied that grounds for the warrant application exist, that magistrate or judge may issue a warrant identifying the property to be seized and describing the specific place to be searched to find the identified property).

11. An arrest warrant is "[a] warrant . . . directing a law-enforcement officer to arrest and bring a person to court." BLACK'S LAW DICTIONARY, *supra* note 10, at 1616. See generally *Steagald v. United States*, 451 U.S. 204, 213 (1981) ("An arrest warrant is issued by a magistrate upon a showing that probable cause exists to believe that the subject of the warrant has committed an offense and thus the warrant primarily serves to protect an individual from an unreasonable seizure.")

12. See, e.g., *Ex parte Burford*, 7 U.S. (3 Cranch) 448, 451–53 (1806) (considering the constitutionality of an arrest warrant and clarifying that probable cause required "good cause certain" to make the arrest).

13. See, e.g., *Carroll v. United States*, 267 U.S. 132, 157 (1925) ("In cases of misdemeanor, a peace officer like a private person has at common law no power of arresting without a warrant except when a breach of the peace has been committed in his presence or there is reasonable ground for supposing that a breach of peace is about to be committed or renewed in his presence.") (quoting 9 HALSBURY'S LAWS OF ENGLAND § 612, at 699 (1st ed. 1907)).

14. *In re Rule of Court*, 20 F. Cas. 1336, 1337 (Bradley, Circuit Justice, C.C.N.D. Ga. 1877) (No. 12,126).

15. *United States v. Maresca*, 266 F. 713, 721 (S.D.N.Y. 1920).

Before 1967, search warrants were a less widely used tool than arrest warrants due to the limitation of the "mere evidence" rule. Under the mere evidence rule, stated most definitively in *Gouled v. United States*,¹⁶ search warrants could be obtained only to seize fruits of crime, instrumentalities of crime, or contraband.¹⁷ In contrast, the government could not obtain a warrant for mere evidence.¹⁸ The Court rooted this limitation in property law: under the Fourth Amendment, the Court held, the government's power was limited to seizing property that the suspect had no right to possess.¹⁹ During this period, the nature of the probable cause inquiry was straightforward. Probable cause was established based on a likelihood that contraband, fruits of crime such as stolen goods, or instrumentalities of crime were located in the place to be searched.²⁰

B. *Warden v. Hayden*

The traditional meaning of warrants for Fourth Amendment law changed considerably in *Warden v. Hayden*,²¹ a decision by Justice Brennan that abolished the mere evidence rule.²² *Hayden* held that warrants could be obtained for evidence just as readily as it could be obtained for contraband or fruits of crime.²³ The Court reasoned that the Fourth Amendment had evolved from its property-based origins to a more general tool of regulating law enforcement that balanced government interests against privacy interests.²⁴ Because the "government has an interest in solving crime," it was reasonable for the government to obtain a warrant for evidence needed to solve those crimes.²⁵ Warrants for mere evidence were reasonable and therefore permitted.²⁶

Hayden's extension of Fourth Amendment warrants to mere evidence created a new problem as to how to define probable cause. Property was contraband or stolen goods apart from how the government planned to use it. In the past, then, probable cause for a search warrant was readily defined in

16. 255 U.S. 298 (1921), *abrogated by* *Warden v. Hayden*, 387 U.S. 294 (1967).

17. According to the Court, a warrant could be obtained only when "the public or the complainant" had a superior claim of property or possession of the item to be seized than the suspect or "when a valid exercise of the police power renders possession of the property by the accused unlawful and provides that it may be taken." *Id.* at 309.

18. *Id.*

19. *Id.*

20. See Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEXAS L. REV. 49, 54-56 (1995) (noting that before the Warren Court, "[t]he Court's cases stressed that law enforcement authorities' power to search was limited to instrumentalities and fruits of the crime or contraband").

21. 387 U.S. 294 (1967).

22. *Id.* at 310.

23. *Id.* at 301-02.

24. *Id.* at 305-07.

25. *Id.* at 306-07.

26. *Id.*

the abstract as a level of cause showing that such items existed in the place to be searched.²⁷ In contrast, whether property counted as “evidence” depended on the context.²⁸ Property could be evidence for one case but not evidence for another.²⁹ The Court responded to this problem by ruling that the probable cause inquiry had to be measured based on a specific set of contemplated crimes and charges.³⁰ “[I]n the case of ‘mere evidence,’” Justice Brennan wrote, “probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction.”³¹ As a result, probable cause had to include both evidence that a particular crime had been committed and that there was evidence of that crime in the place to be searched.³²

C. *Camara v. Municipal Court*

Although *Warden v. Hayden* signaled a major change in the traditional meaning of warrants, the more radical shift occurred soon after in *Camara v. Municipal Court*.³³ *Camara* reconsidered a line of Supreme Court precedents on the Fourth Amendment governing health and safety inspectors who wished to enter homes to check for code violations.³⁴ This was a major issue in American cities at the time because of concerns about urban slums and the prospects of urban renewal.³⁵ Just eight years earlier, in *Frank v. Maryland*,³⁶ the Supreme Court had upheld these warrantless housing inspections on the ground that they were necessary to enforce important health and safety laws.³⁷ The government had a pressing need to inspect homes for violations, the Court reasoned, and that ability “would be greatly hobbled by the blanket requirement of the safeguards necessary for a search of evidence of criminal acts.”³⁸

In *Camara*, the Court overruled *Frank* and held that a warrant was required for such inspections.³⁹ But there was a catch: the warrant that was required was unlike any warrant previously known. Writing for the Court,

27. See, e.g., *Steagald v. United States*, 451 U.S. 204, 213 (1981) (“A search warrant . . . is issued upon a showing of probable cause to believe that the legitimate object of a search is located in a particular place . . .”).

28. *Hayden*, 387 U.S. at 301–02.

29. *Id.* at 302.

30. *Id.* at 307.

31. *Id.*

32. *Id.* at 309.

33. 387 U.S. 523 (1967).

34. *Id.* at 527–28.

35. See, e.g., Wendell E. Pritchett, *The “Public Menace” of Blight: Urban Renewal and the Private Uses of Eminent Domain*, 21 YALE L. & POL’Y REV. 1, 31–32 (2003) (detailing the rise of government intervention in urban revitalization).

36. 359 U.S. 360 (1959), overruled by *Camara v. Mun. Court*, 387 U.S. 523 (1967).

37. *Id.* at 372–73.

38. *Id.* at 372.

39. *Camara*, 387 U.S. at 528.

Justice White reasoned that the core of the Fourth Amendment was reasonableness, and that reasonableness required a balancing of interests between the government's need for the search and the citizen's need for privacy and security.⁴⁰ Although the government needed a warrant based on probable cause to search a home, *what there was probable cause to believe* could vary based on what government interest was at play.⁴¹ "To apply this standard," Justice White explained, "it is obviously necessary first to focus upon the governmental interest which allegedly justifies official intrusion upon the constitutionally protected interests of the private citizen."⁴²

From this perspective, the traditional search warrant of criminal law was merely one application of a general interest balancing that happened to occur in criminal cases:

[I]n a criminal investigation, the police may undertake to recover specific stolen or contraband goods. But that public interest would hardly justify a sweeping search of an entire city conducted in the hope that these goods might be found. Consequently, a search for these goods, even with a warrant, is "reasonable" only when there is "probable cause" to believe that they will be uncovered in a particular dwelling.⁴³

Justice White then applied that framework to the governmental interest of maintaining health and safety standards pursuant to city codes. "In determining whether a particular inspection is reasonable . . .," Justice White wrote, "the need for the inspection must be weighed in terms of these reasonable goals of code enforcement."⁴⁴ Justice White reviewed the social-science literature on public safety inspections and concluded that it would be reasonable to require warrants but allow those warrants to be issued to search entire areas of buildings based on a proof of need to do so.⁴⁵ Such a system would balance the governmental interest in maintaining health and safety standards with the interest in security from a government search.⁴⁶

D. *United States v. United States District Court*

The first case applying the general balancing approach to the national security setting was *United States v. United States District Court (Keith)*,⁴⁷ generally known as the *Keith* case because the district judge was Judge

40. *Id.* at 536-39.

41. *Id.* at 534.

42. *Id.*

43. *Id.* at 535.

44. *Id.*

45. *Id.* at 535-39.

46. *Id.* at 539.

47. 407 U.S. 297 (1972).

Damon Keith.⁴⁸ The issue in *Keith* was whether the Fourth Amendment required the government to obtain a warrant to conduct wiretapping of a U.S. citizen for domestic national security purposes.⁴⁹ In an opinion by Justice Powell, the Court balanced the interests of national security against domestic threats versus the benefits of a warrant requirement and concluded that it was reasonable to require the government to obtain a warrant before such monitoring occurred.⁵⁰ On one hand, the governmental interest in protecting the country was a vital one:

It has been said that “[t]he most basic function of any government is to provide for the security of the individual and of his property.” And unless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered.⁵¹

On the other hand, protection from arbitrary government searches was also critical, especially in light of the threat to privacy and First Amendment values presented by a regime of warrantless searches when the government itself is a potential target.⁵² Balancing the two interests, the Court concluded that a warrant requirement was a reasonable accommodation: “Although some added burden will be imposed upon the Attorney General, this inconvenience is justified in a free society to protect constitutional values.”⁵³

Tracking *Camara*, however, the Court noted that the “warrant” required did not need to be an ordinary criminal law warrant.⁵⁴ “[D]omestic security surveillance may involve different policy and practical considerations from the surveillance of ‘ordinary crime,’” Justice Powell acknowledged.⁵⁵ Specifically, a reasonable warrant system could be based on different standards of probable cause and particularity than a criminal law warrant:

Different standards [for obtaining warrants] may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.⁵⁶

In other words, the Court required a warrant because it was reasonable to require a warrant, but the warrant that was required was whatever standard

48. Tracey Maclin, *The Bush Administration's Terrorist Surveillance Program and the Fourth Amendment's Warrant Requirement: Lessons from Justice Powell and the Keith Case*, 41 U.C. DAVIS L. REV. 1259, 1263 n.9 (2008).

49. *Keith*, 407 U.S. at 299.

50. *Id.* at 321.

51. *Id.* at 312 (quoting *Miranda v. Arizona*, 384 U.S. 436, 539 (1966) (White, J., dissenting)).

52. *Id.* at 316–20.

53. *Id.* at 321.

54. *Id.* at 322.

55. *Id.*

56. *Id.* at 322–23.

was reasonable to require. This is reasonableness piled on top of reasonableness: it essentially permits the Court to impose a warrant requirement if it can devise a standard for a warrant that makes such a requirement a workable one.

Cases like *Keith* and *Camara* are generally understood as important civil liberties cases.⁵⁷ The Supreme Court expanded the Warrant Clause in these cases, inserting the ex ante judicial review where it had not been inserted before. But the key for our purposes is realizing *how* the Court expanded the Clause's reach. The key move was to make the Warrant Clause a tool of double-barreled reasonableness: warrants are required when a warrant requirement would be reasonable, and the showing required to obtain the warrant is whatever showing would be reasonable to show.

III. How the History of the Warrant Standard Explains the Narrow Warrant Clause in National Security Cases

The Supreme Court's expansion of the Warrant Clause in the late 1960s and early 1970s offers a potentially expansive rationale for requiring warrants that could apply in a wide range of settings in the national security context. Later courts have not applied it this way, however. Although the Supreme Court has not revisited the Warrant Clause in the national security setting since *Keith*, lower courts have for the most part construed the warrant requirement narrowly. For example, lower courts have rejected a warrant requirement for foreign intelligence surveillance,⁵⁸ rejected a warrant requirement for surveillance outside the United States,⁵⁹ and approved the relaxed statutory warrant standard for national security monitoring introduced by the USA PATRIOT Act of 2001.⁶⁰ But why? Why have the

57. See, e.g., Maclin, *supra* note 48, at 1263, 1288 (describing *Keith*'s pro-warrant holding as "remarkable" and stating that "*Camara* would subsequently be interpreted as solidifying the warrant requirement as a core precept in Fourth Amendment law").

58. See, e.g., *United States v. Truong Dinh Hung*, 629 F.2d 908, 914 (4th Cir. 1980) ("[B]ecause of the need of the executive branch for flexibility, its practical experience, and its constitutional competence, the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance."); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) ("Foreign security wiretaps are a recognized exception to the general warrant requirement . . ."); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir. 1974) (en banc) (holding that no warrant was required due to the trial court's finding that the surveillance in question was "conducted . . . solely for the purpose of gathering foreign intelligence information"); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973) ("[T]he President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence."). *But see* *Zweibon v. Mitchell*, 516 F.2d 594, 614 (D.C. Cir. 1975) ("[A] warrant must be obtained before a wiretap is installed on a domestic organization that is neither the agent of nor acting in collaboration with a foreign power, even if the surveillance is . . . in the name of foreign intelligence gathering for protection of the national security.").

59. See *In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157, 167 (2d Cir. 2008) (holding that the Warrant Clause does not apply outside the United States).

60. See *In re Sealed Case*, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) ("[W]e think the procedures and government showings required under FISA, if they do not meet the minimum Fourth

lower courts interpreted the Warrant Clause narrowly in national security cases after *Keith*?

This Part offers a pragmatic argument for why the Warrant Clause has been applied narrowly in the national security setting. The core problem is that the malleable Warrant Clause requires courts to consider whether a warrant regime would be reasonable over a hypothetical set of facts. The court must imagine a set of hypothetical investigations, and it then must consider how those investigations would hypothetically operate with a hypothetical warrant requirement and whether that hypothetical regime would be reasonable. This is different from the usual question in Fourth Amendment cases. In traditional Fourth Amendment cases, the government will conduct a search or seizure, and the court must then say if that particular search or seizure was reasonable.⁶¹ The review is *ex post*, and it is limited to a specific set of facts.⁶² The malleable Warrant Clause forces judges to do something quite different. Courts must consider how national security investigations operate generally, and they then must ask how a hypothetical warrant requirement would operate within that understanding.

Courts are ill-equipped to answer such questions for four major reasons. The first is the chicken-and-egg problem: courts do not know what kind of warrant they must imagine operating because the kind of warrant is itself left open. Second, the Judiciary cannot know whether the elected branches would set up courts with expert judges or with jurisdiction to issue those warrants, making it difficult for them to assess how such a warrant requirement would work. Third, courts cannot know the technology of surveillance that will apply or whether diplomatic agreements will harmonize the different legal regimes, making it hard to know how warrants would be executed. And fourth, uncertainty as to the law of when national security investigations trigger the Fourth Amendment at all leaves courts uncertain as to what set of facts they will be balancing. Faced with these considerable uncertainties, courts have been and will continue to be tentative. The Warrant Clause may be in play in theory, but its actual reach in national security cases will remain modest.

A. *The Chicken-and-Egg Problem*

The first reason why the courts have applied the warrant requirement narrowly is what I call the chicken-and-egg problem. There are two basic questions raised by a regime of surveillance pursuant to a warrant: whether a

Amendment warrant standards, certainly come close. We, therefore, believe firmly . . . that FISA as amended is constitutional because the surveillances it authorizes are reasonable.”).

61. See, e.g., *Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (determining that an already executed search warrant was “plainly invalid”).

62. See, e.g., *id.* (“The warrant in this case complied with the first three [constitutional] requirements: It was based on probable cause and supported by a sworn affidavit, and it described particularly the place of the search. On the fourth requirement, however, the warrant failed altogether.”).

warrant is required and what standard the government must satisfy to obtain a warrant. Under the approach to warrants articulated in *Keith*; however, each is based on the other. Whether a warrant is required is based on whether requiring a warrant is workable, but that depends on what standard is required for obtaining a warrant.⁶³ On the other hand, what standard is required for obtaining a warrant depends on what kind of standard would make a warrant standard workable.⁶⁴

This raises an obvious difficulty: Which comes first, the requirement or the standard? It is akin to asking if you can afford a new car, with the caveat that the price of the car depends on what you can afford. Whether you can afford the car cannot be answered because the inquiry is circular: it depends on the price, which depends on what you can afford, which depends on the price, and so on. It is turtles all the way down.⁶⁵

The same goes for national security warrants. When asked to answer whether the Fourth Amendment requires a warrant for a particular kind of national security monitoring, a court will not know what kind of warrant is at issue. A warrant is not required so long as a warrant requirement would be impractical,⁶⁶ but the court does not know what kind of warrant the court must evaluate to determine its practicability.⁶⁷ Again, it is like asking if you can afford a car but not disclosing the price: the honest answer is that the problem is indeterminate and cannot be answered on the facts provided. Faced with this kind of uncertainty, most courts are likely to be cautious.

For the most part, the most courts are likely to do in such a setting is (a) require a warrant but then leave the standard for obtaining the warrant unclear or (b) evaluate whether an existing and established statutory warrant system meets constitutional muster. *Keith* is an example of the former: the Supreme Court required a warrant, but then left open the question of what kind of warrant was actually required.⁶⁸ It was up to Congress to act and to choose a type of warrant that it would require. The decision of the Foreign

63. See *supra* notes 47–57 and accompanying text.

64. See *supra* notes 47–57 and accompanying text.

65. See *Rapanos v. United States*, 547 U.S. 715, 754 n.14 (2006) (citing CLIFFORD GEERTZ, *THE INTERPRETATION OF CULTURES* 28–29 (1973)). The Court has offered one variation of this story:

[A]n Eastern guru affirms that the earth is supported on the back of a tiger. When asked what supports the tiger, he says it stands upon an elephant; and when asked what supports the elephant he says it is a giant turtle. When asked, finally, what supports the giant turtle, he is briefly taken aback, but quickly replies “Ah, after that it is turtles all the way down.”

Id.

66. See *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 322–23 (1972) (holding that because domestic security surveillance may involve different policy and practical considerations, the warrant application may vary according to the governmental interest).

67. *Id.*

68. See *id.* (holding that the warrant application may vary with the governmental interest and the citizen rights deserving protection without specifying what type of warrant is required).

Intelligence Court of Review in *In re Sealed Case*⁶⁹ is an example of the latter: the Court could review the choices made by Congress for the standard required to obtain a warrant and then pronounce it legally acceptable or not.⁷⁰ In both settings, the Warrant Clause played a relatively modest role. The main work in creating the law of foreign intelligence surveillance was up to Congress rather than the courts.⁷¹

B. The Judiciary Cannot Control Expertise or Jurisdiction Ex Ante

The second reason the Warrant Clause will tend to play a modest role in national security investigations is that whether a warrant system is reasonable depends on legislative choices that determine the Judiciary's competence and ability to issue warrants. Consider two variables in particular: whether the courts have expertise in national security issues and whether a warrant can be obtained to search that location. Both of these variables have been cited by courts as grounds for rejecting warrant requirements in national security cases.⁷² But the real difficulty with these two variables is not that they suggest warrant requirements are impractical but rather that they depend on legislative action. The reasonableness of the warrant requirement hinges on legislative choices outside the Judiciary's control.

Consider the question of expertise. In *United States v. Truong Dinh Hung*,⁷³ the Fourth Circuit mostly rejected a warrant requirement for foreign intelligence surveillance primarily on the ground that judges lack the relevant expertise in national security issues: "[W]hile the courts possess expertise in making the probable cause determination involved in surveillance of suspected criminals, the courts are unschooled in diplomacy and military affairs, a mastery of which would be essential to passing upon an executive branch request that a foreign intelligence wiretap be authorized."⁷⁴ The problem with this argument is that the expertise of a judge is a variable. It depends on the variable of the judge's training, schooling, and experience. While many

69. 310 F.3d 717 (FISA Ct. Rev. 2002).

70. See *id.* at 736–46 (analyzing the consistency of FISA with the Fourth Amendment and finding no constitutional violation).

71. See *Keith*, 407 U.S. at 323–24 (noting that the Court does not attempt to guide congressional judgments and that approval of domestic security surveillance may be made in accordance with Congress's prescribed standards); *In re Sealed Case*, 310 F.3d at 736 (holding that FISA as amended did not require the Government to show that its main purpose of surveillance was not criminal prosecution).

72. See, e.g., *In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157, 168–71 (2d Cir. 2008) (determining that "[t]he question of whether a warrant is required for overseas searches of U.S. citizens has not been decided by the Supreme Court, by our Court, or . . . by any of our sister circuits" and ultimately holding that "the Fourth Amendment's Warrant Clause has no extraterritorial application and that foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment's requirement of reasonableness"); *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) ("[T]he judiciary is largely inexperienced in making the delicate and complex decisions that lie behind foreign intelligence surveillance.").

73. 629 F.2d 908 (4th Cir. 1980).

74. *Id.* at 913–14.

judges will not have the relevant experience, Congress can ensure that some will.

Our experience with the Foreign Intelligence Surveillance Court (FISC) is instructive. Judges are appointed to the FISC by the Chief Justice for seven-year terms.⁷⁵ To ensure that the FISC judges have expertise, the Chief Justice can select judges whose backgrounds and experience suggest they have experience or aptitude in surveillance and national security issues. The current membership of the FISC suggests that they were not chosen at random. Among its eleven current members, five have served as officers in the military.⁷⁶ A recent member of the court authored a widely respected treatise on electronic surveillance law.⁷⁷ Even apart from their past experience, the seven-year appointment to the FISC allows judges to develop expertise. The long-term appointment allows judges on the FISC to specialize in the topic, master the methods, and generally obtain an understanding of the Executive worldview.

My point is not that concerns of expertise are meritless. They are not. Rather, my point is that expertise is somewhat contingent on matters outside the control of the court trying to measure judicial expertise. The reality may be that judges will have expertise if Congress and the President value expertise and create a specialized court staffed with expert judges. But the court asked to assess judicial expertise cannot know what the other branches might do. The reviewing court cannot know how to measure the variable without future input from the other branches.

The same point goes for jurisdiction to issue a warrant. In a recent decision, *In re Terrorist Bombings of U.S. Embassies*,⁷⁸ the Second Circuit held that the Warrant Clause of the Fourth Amendment does not apply at all to searches or surveillance that occur outside the United States.⁷⁹ Part of the court's reasoning focused on "the absence of a mechanism for obtaining a U.S. warrant" to search overseas.⁸⁰ Indeed, traditionally warrants have only been allowed to search for property in that district.⁸¹ Warrants to search and seize property abroad therefore have not been authorized.

75. 50 U.S.C. § 1803(a), (d) (2006).

76. Presiding Judge John Bates served in the Army from 1968–1971. Malcolm Howard was in the Army from 1962–1972. George Kazen was in the Air Force from 1962–1965. Frederick Scullin was an infantry commander in Vietnam. Roger Vinson was a naval aviator from 1962–1968. Federal Judicial Center., Biographical Directory of Federal Judges, <http://www.fjc.gov/public/home.nsf/hisj> (search by each judge's last name).

77. Judge James G. Carr was a member of the FISC from 2002–2008. American Constitution Society for Law and Policy, The Honorable James G. Carr, <http://www.acslaw.org/node/15114>. He is the primary author of the noted treatise, *The Law of Electronic Surveillance*. JAMES G. CARR & PATRICIA L. BELLIA, *THE LAW OF ELECTRONIC SURVEILLANCE* (2002).

78. 552 F.3d 157 (2d Cir. 2008).

79. *Id.* at 159.

80. *Id.* at 172.

81. See FED. R. CRIM. P. 41(b)(1) (“[A] magistrate judge . . . has authority to issue a warrant to search for and seize a person or property located within the district . . .”).

That decision appears to be a matter of legislative choice rather than constitutional command, however. In the same year as *In re Terrorist Bombings*, a new federal rule went into effect that permits a magistrate judge to issue warrants in “United States diplomatic or consular mission[s] in a foreign state.”⁸² Although the rule is narrow in that it applies only to properties controlled by the United States, it seems to reflect the broader point that Congress could—if it wished—authorize U.S. judges to issue warrants authorizing foreign searches.

If the reasonableness of a warrant regime plausibly depends, at least in part, on whether judges have been authorized to issue warrants to conduct those searches, then judges called on to determine the reasonableness of a warrant regime face a problem. Just as they cannot predict whether Congress will create a specialized court, they cannot predict whether Congress will create the authority to issue the warrants that would make a warrant requirement reasonable.

C. *Changing Technology and Diplomatic Agreements*

Changing technology and diplomatic agreements present a third problem for assessing the reasonableness of a warrant regime. The reasonableness of a warrant regime depends on the practical question of how warrants are executed. Justice Kennedy’s concurring opinion in *United States v. Verdugo-Urquidez*⁸³ is instructive. Justice Kennedy’s opinion considered some of the practical problems that would accompany a warrant requirement for searches outside the United States:

The absence of local judges or magistrates available to issue warrants, the differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad, and the need to cooperate with foreign officials all indicate that the Fourth Amendment’s warrant requirement should not apply [to searches outside the United States] as it does in this country.⁸⁴

These concerns are sensible if you assume a physical search and the need for a local warrant that is obtained independently of a U.S. warrant. But if you change some of these assumptions, some of those concerns change as well.

Consider a foreign search that occurs by way of wiretapping or other direct access to electronic communications. Perhaps the United States accesses the communications from a monitoring site outside the United States.⁸⁵ Perhaps the foreign-to-foreign communications are routed through

82. *Id.* R. 41(b)(5)(B).

83. 494 U.S. 259 (1990).

84. *Id.* at 278 (Kennedy, J., concurring).

85. See, e.g., Lawrence D. Sloan, Note, *ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 DUKE L.J. 1467, 1504 (2001) (warning that the “incidentally acquired information” rule, which permits the U.S. government to accept incidentally

the United States in the course of delivery.⁸⁶ Perhaps the communications are routed through foreign computers owned by a U.S. company that has close relations with the U.S. government. Or perhaps the communications are stored on a remote server, and U.S. officials can access the foreign server directly and download the targeted files.⁸⁷ In any of these instances, the government will access the communications directly: it does not need any help from foreign governments or foreign companies. While there may be sound diplomatic reasons not to act unilaterally,⁸⁸ often unilateral action will be possible. Further, accessing the communications might just require the flipping of a switch. In that environment, the practical concerns mentioned by Justice Kennedy no longer seem to provide a practical limitation on a warrant requirement.

Mutual legal assistance treaties and international agreements can also address some of those concerns. For example, the Council of Europe Cybercrime Convention attempts to harmonize the laws governing access to electronic communications among the signatory countries.⁸⁹ Under Section 2 of the Convention, each country must have procedural laws that roughly replicate the Electronic Communications Privacy Act,⁹⁰ which regulates the privacy of Internet communications in the United States. There must be rules governing access to subscriber information held by Internet Service Providers,⁹¹ rules for access to content information,⁹² rules governing search and seizure of stored computer data,⁹³ and the like. No two countries have to adopt the same standards for access, of course. But each country does need to have a roughly parallel legal structure so as to facilitate interaction in investigations that cross borders.⁹⁴

acquired information from foreign governments, could be used as a subtle circumvention of the law to monitor activity by U.S. citizens).

86. See generally *id.* at 1477–78 (describing how a significant amount of global Internet traffic is routed through the United States in the course of delivery even if that traffic does not originate or reach its final destination inside the United States).

87. See, e.g., *United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026, at *1 (W.D. Wash. May 23, 2001) (chronicling an incident where U.S. agents used the defendant's password to log in to a Russian server from the United States and download files belonging to the defendant).

88. See, e.g., Note, *Predictability and Comity: Toward Common Principles of Extraterritorial Jurisdiction*, 98 HARV. L. REV. 1310, 1320 (1985) (“This entire approach rests on a fallacy: even if we assume that the United States’ interests are legitimate, it does not necessarily follow that the United States is justified in acting unilaterally to achieve them.”).

89. See Anne Flanagan, *The Law and Computer Crime: Reading the Script of Reform*, 13 INT’L J.L. & INFO. TECH. 98, 109 (2005) (“[The Convention] is the first international treaty exclusively addressing issues surrounding computers and crime.”).

90. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered titles of U.S.C.).

91. Council of Europe, Convention on Cybercrime, art. 20, *opened for signature* Nov. 11, 2001, Europ. T.S. No. 185.

92. *Id.* art. 21.

93. *Id.* art. 19.

94. *Id.* art. 23–25.

Again, my argument is not that concerns over the diversity of legal regulation don't matter. Rather, it is that the significance of these concerns hinges on matters outside the Judiciary's control. Judges cannot make the President and Congress act to create a mutual legal assistance treaty or to join or reject an international convention on legal harmonization. Nor can judges predict whether the laws are likely to become more or less harmonized over time. As a result, they cannot readily predict to what extent the practical concerns with harmonization actually render a warrant requirement reasonable or unreasonable.

D. Legal Uncertainty as to When the Fourth Amendment Is Triggered

The fourth problem with assessing the reasonableness of a warrant regime in the national security area is uncertainty as to how the law applies to common facts. National security investigations rarely come before the courts, and that means that there are few opinions (at least few published opinions⁹⁵) on some of the most important questions. For example, it remains highly uncertain precisely how much voluntary contact with the United States a person who is not a citizen or permanent resident alien must have to get Fourth Amendment rights.⁹⁶ It remains uncertain how the Fourth Amendment applies to access to streams of communications when the government believes the communications are among individuals who have no Fourth Amendment rights if it later turns out that the government's belief was wrong. The Fourth Amendment rights of U.S. citizens abroad also remain uncertain, with some courts looking to foreign law to identify the standard⁹⁷ and others looking to general reasonableness in terms of a balance between privacy and government interests.⁹⁸

The effect of these uncertainties is to create significant uncertainty as to what type of facts the court needs to balance when considering whether a warrant requirement would be reasonable. Imposing a warrant requirement means imposing it over a set of facts. However, the uncertainty as to how the Fourth Amendment applies to these common fact patterns means that courts cannot know the set of facts to which they would apply the warrant requirement. Again, the uncertainty in the law counsels modesty in applying

95. There is a possibility that the FISC has developed a secret body of Fourth Amendment law that governs the work of the FISC but that is not known to outsiders. As outsiders, we cannot know whether that body of law exists or what it says.

96. *See, e.g., United States v. Verdugo-Urquidez*, 494 U.S. 259, 274–75 (1990) (refusing to extend Fourth Amendment protections to non-U.S. citizens living in different countries and saying that if such protections are going to be enacted it will be through the “political branches” by other means).

97. *See, e.g., United States v. Barona*, 56 F.3d 1087, 1096 (9th Cir. 1995) (using the fact that Danish law was complied with to support the holding that Fourth Amendment violations did not occur).

98. *See, e.g., In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157, 167–71 (2d Cir. 2008) (listing various reasons to apply the reasonableness standard in such contexts).

a warrant requirement: courts cannot be sure how the warrant requirement would apply because they would not know the background set of facts over which the rule would be enforced.

IV. Conclusion

The surprisingly malleable Warrant Clause was originally understood as a boon to civil liberties.⁹⁹ In cases like *Camara* and *Keith*, the Supreme Court stepped in and imposed a warrant requirement where one had not been applied before. In expanding the Warrant Clause, however, the Court also watered it down: the malleable approach to reasonableness leaves so much uncertain that the Warrant Clause exists in theory but will be interpreted cautiously in practice. Courts do not have the tools or know the facts needed to make predictions as to whether a warrant requirement would be reasonable except in very limited circumstances. Boldly going forth and imposing a constitutional warrant requirement in such circumstances would be reckless absent significant judicial certainty that such a requirement would in fact be reasonable. As a result, the Warrant Clause tends to play a modest role in national security investigations. It can spark action, leaving the details up to the legislature, or it can ratify or reject a specific legislative working scheme. But it cannot play the same strong role in national security cases that it has traditionally played in criminal investigations.

99. See *supra* note 57 and accompanying text.

The Argument Against Technology-Neutral Surveillance Laws

Paul Ohm*

Introduction

Should Congress write tech-specific or tech-neutral laws? Those who have considered this question have almost always chosen neutrality: laws should refer to the effects, functions, or general characteristics of technology, but never to a particular type or class of technology.¹ Those who espouse tech neutrality come from across the political and ideological spectrum and embrace tech neutrality dogmatically, often referring to it as a “principle,” one presumably violated only in exceptional circumstances for the most compelling reasons.²

But a close examination of the arguments supporting tech neutrality reveals many underappreciated flaws. At least three arguments support tech neutrality—consistency, the need to avoid underinclusiveness, and the recognition of institutional shortcomings—but each is contingent and rebuttable, and in many situations does not apply.

While other scholars have called Congress’s blind adherence to the principle of tech neutrality into question,³ none have explored the neutrality of laws regulating government search and surveillance. This rich, important context bears close scrutiny because the path of surveillance law so often follows the twists and turns of evolving technology.⁴ Moreover, since 9/11, Congress has more than once replaced tech-specific surveillance laws with tech-neutral ones: for example, with the USA PATRIOT Act⁵ Congress

* Associate Professor of Law, University of Colorado Law School. I thank Professor Bobby Chesney and the editors of the Texas Law Review for the invitation to participate. I also thank the participants at both the Symposium and the University of Colorado workshop series for their comments. In particular, I would like to thank William Boyd, Joe Feller, Susan Freiwald, Jennifer Granick, Lisa Graves, Marcia Hoffman, Clare Huntington, Orin Kerr, Derek Kiernan-Johnson, Sarah Krakoff, Michael Kwun, Jon Michaels, Scott Moss, Helen Norton, John Radsan, Carolyn Ramsey, Andrew Schwartz, Harry Surden, and Wendy Seltzer for their comments.

1. See, e.g., *infra* notes 29–30 and accompanying text.

2. See *infra* note 36 and accompanying text.

3. See Lyria Bennett Moses, *Recurring Dilemmas: The Law’s Race to Keep Up with Technological Change*, 2007 U. ILL. J.L. TECH. & POL’Y 239, 239 (complaining that tech-neutral drafting may not be effective as technology changes); Chris Reed, *Taking Sides on Technology Neutrality*, 4 SCRIPT-ED 263, 282–84 (2007) (advocating a three-step process lawmakers should undergo when deciding between tech-neutral and tech-specific legislation).

4. See, e.g., John Schwartz, *Debate over Full-Body Scans vs. Invasion of Privacy Flares Anew After Incident*, N.Y. TIMES, Dec. 29, 2009, at A14 (discussing potential legislation to regulate the use of newly developed full-body scanners in airports).

5. Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered titles of U.S.C.).

brought neutrality to the Pen Register and Trap and Trace Devices Act⁶ (Pen Register Act), and through the Protect America Act⁷ (PAA) it did the same for the Foreign Intelligence Surveillance Act⁸ (FISA).

We should worry about this trend because the arguments in favor of tech neutrality are especially misguided in the surveillance context. When it comes to surveillance, every argument supporting tech neutrality can be met with a powerful counterargument: Tech-neutral laws often force consistency, even when inconsistency is preferable; they avoid underinclusiveness by permitting overinclusiveness; and they address Congress's supposed institutional shortcomings by cutting Legislative oversight over surveillance, even though history has taught us to beware the surveillance of an unchecked Executive. Given the deep flaws in the arguments for tech neutrality in the surveillance context, we should stop treating tech neutrality as a principle and instead treat it as a choice.

Finally, the blind adherence to the principle of tech neutrality pushes Congress away from the many benefits of tech specificity. Most importantly, a tech-specific surveillance law, even one imposing few constraints on the agencies conducting surveillance, forces the Executive Branch to consult with Congress whenever technology changes in significant ways, which might help offset the troubling culture of secrecy in national security policy by bringing broader, more participatory democratic oversight to the conduct of national surveillance. Also, because technology evolves so rapidly and constantly, tech-specific surveillance laws operate as a technology sunset, expiring not on some arbitrarily defined timetable, but whenever the circumstances demand. Both of these benefits increase the Legislature's role in national surveillance and national security debates and restore checks against the Executive's power in ways that might have helped avoid some of the surveillance abuses and excesses of the recent past.

This Article proceeds in three Parts, offering, in turn, the best arguments for tech neutrality (Part I), the underappreciated counterarguments to those arguments (Part II), and the case for tech specificity (Part III). Ultimately, this Article tries to counter the pervasively held attitude that tech-specific laws are indefensible mistakes to be avoided. Quite often, tech specificity is the wiser course—the best way to balance the government's need to provide security with the right to privacy.

6. 18 U.S.C. §§ 3121–3127 (2006).

7. Pub. L. No. 110-55, 121 Stat. 552 (2007) (to be codified at 50 U.S.C. §§ 1803, 1805a–1805c).

8. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended in scattered titles of U.S.C.).

I. Tech-Neutral Laws

A. *Defining Tech Neutrality*

Whenever Congress writes a law to address a problem caused by technology, it must decide whether to draft tech-neutral or tech-specific provisions. Tech-neutral provisions refer to technology in general, vague, open-textured terms that specify purposes, effects, functions, and other general characteristics. While Congress has used tech neutrality for surveillance law inconsistently, for decades it has embraced neutral drafting in other tech-heavy fields such as telecommunications⁹ and copyright. Under the Copyright Act, for example, copies are defined in part as “material objects . . . in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.”¹⁰

In contrast, tech-specific provisions refer to specific types or classes of technologies. For example, the Pen Register Act, a surveillance law, once applied only to “a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached.”¹¹ In the USA PATRIOT Act, Congress replaced this tech-specific definition with a tech-neutral one that broadly covers all “dialing, routing, addressing, or signaling information.”¹² We will revisit this example later in the Article.¹³

Most tech-centric laws lie along a spectrum from tech specificity to tech neutrality with few as close to either endpoint as the laws just cited. Sometimes it can be tricky to tell near which end of the spectrum a statute falls. A definition may seem tech specific on first blush because it lists specific types of technologies, but sometimes the point of such a list is to exhaust possibilities, covering the definitional waterfront, signaling that the list is meant to cover everything neutrally. For example, the Computer Fraud and Abuse Act—a Federal anti-computer-hacking law—defines a computer to mean “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”¹⁴ Despite providing a long list of specific types of technology, Congress intended this definition to

9. See Reed, *supra* note 3, at 264 (recognizing that “technology neutrality has continued to be a pervasive concept” in telecommunications policy).

10. 17 U.S.C. § 101 (2006).

11. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, sec. 301, § 3126(3), 100 Stat. 1848, 1871.

12. USA PATRIOT Act of 2001, Pub. L. No. 107-56, sec. 216, 115 Stat. 272, 290 (codified at 18 U.S.C. § 3127(3) (2006)).

13. See *infra* notes 147–52 and accompanying text.

14. 18 U.S.C. § 1030(e)(1) (2006).

have a broadly neutral meaning, and indeed the Seventh Circuit has interpreted it to cover not only laptop and desktop computers but “[e]very cell phone and cell tower[,] . . . every iPod, every wireless base station in the corner coffee shop, and many another gadget.”¹⁵

Congress must often choose between tech neutrality and specificity when it drafts surveillance laws because the great challenge of surveillance is keeping up with the latest advances in technology. Over the decades, it has written surveillance laws that fit at different points along the spectrum. Consider one law in particular, the Wiretap Act,¹⁶ and take a single, complex subsection of this Act, 18 U.S.C. § 2511(2)(g), which lists exceptions to the general prohibition on wiretapping, and this subsection provides a menagerie of examples from across the specificity spectrum. Under § 2511(2)(g), it is not an illegal wiretap to intercept electronic communications that are “readily accessible to the general public”¹⁷—a classically tech-neutral rule—radio communications “transmitted by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services”¹⁸—a mostly tech-specific rule—or communications, “the transmission of which [are] causing harmful interference” to another radio “to the extent necessary to identify the source of such interference”¹⁹—which seems to fall somewhere in between.

Through the first few technological epochs of electronic surveillance—from the earliest telephone wiretaps,²⁰ to the spike mikes²¹ and room bugs²² of the mid-twentieth century, up until the early days of computer-network surveillance—Congress wrote many tech-specific surveillance laws. My strong sense is that in the past decade or so, it has switched to writing only tech-neutral ones. As one example, the precursors to the tech-specific Wiretap Act provisions listed above were included in the original 1968

15. *United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005).

16. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211–23 (codified as amended at 18 U.S.C. §§ 2510–2520, 47 U.S.C. § 605 (2006)).

17. 18 U.S.C. § 2511(2)(g)(i) (2006).

18. *Id.* § 2511(2)(g)(ii)(III).

19. *Id.* § 2511(2)(g)(iv).

20. *See Olmstead v. United States*, 277 U.S. 438, 456–57 (1928) (describing the wiretap as small wires inserted into the telephone lines coming from the petitioners’ houses).

21. *See Silverman v. United States*, 365 U.S. 505, 506–07 (1961) (describing the instrument used as a microphone with a spike attached to it that was inserted into the house to become a “conductor of sound”); *Goldman v. United States*, 316 U.S. 129, 131 (1940) (“They had with them another device . . . having a receiver so delicate as, when placed against the partition wall, to pick up sound waves . . .”).

22. *See Katz v. United States*, 389 U.S. 347, 348 (1967) (describing the device used as capable of intercepting communications while being placed outside of a structure).

Wiretap Act,²³ while the tech-neutral “readily accessible” provision was added much more recently.²⁴

B. Tech Neutrality in National Security Surveillance Law

Those who urge Congress to expand surveillance authorities to protect national security often argue for tech-neutral surveillance laws. For example, John Yoo and Eric Posner applauded the USA PATRIOT Act’s amendments to FISA for embracing tech neutrality.²⁵ Thanks to the USA PATRIOT Act, “FISA warrants . . . are now technology-neutral . . . [and] allow continuing surveillance of a terrorist target even if he switches communication devices and methods.”²⁶

While Yoo and Posner lauded the shift to a tech-neutral FISA warrant standard, others remained dissatisfied about lingering tech specificity in the law, even after the USA PATRIOT Act. In particular, in the middle part of the first decade of the twenty-first century, Executive Branch officials pressed Congress to fix one form of lingering specificity in FISA—the way it treated communications bouncing through satellites differently than communications carried on fiber-optic cables.²⁷ Under the widely accepted interpretation of the statute’s definitions, if the NSA wanted to monitor the communications of a foreigner (or, to use the statute’s term, a non-“United States person”) located outside the United States, it faced significant procedural hurdles if the communications happened to travel over a fiber-optic cable and almost no hurdles if they traveled via satellite.²⁸

23. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, sec. 802, § 2511(2)(a)–(b), 82 Stat. 197, 214.

24. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, sec. 101(b)(4), 100 Stat. 1848, 1850.

25. See John Yoo & Eric Posner, *The Patriot Act Under Fire*, AEI: ON THE ISSUES, Dec. 1, 2003, <http://www.aei.org/issue/19661> (describing tech neutrality as a “common-sense adjustment[]” of necessity).

26. *Id.*

27. See, e.g., *Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 27–28 (2007) [hereinafter *Modernization of FISA*] (statement of Kenneth L. Wainstein, Assistant Att’y Gen. of National Security, United States Department of Justice) (describing the distinction running throughout FISA between wire communications and radio communications).

28. To state the complicated argument concisely, under the definition of “electronic surveillance,” FISA treats surveillance of “wire communications” differently than it treats surveillance of “radio communications.” Compare 18 U.S.C. § 1801(f)(2) (2006) (defining “electronic surveillance” to include wire communications acquired without regard to intent or a reasonable expectation of privacy), with *id.* § 1801(f)(3) (requiring intentional acquisition of the transmission and a reasonable expectation of privacy for acquisitions of radio transmissions to constitute electronic surveillance). Surveillance of radio is not regulated by FISA unless, among other things, “both the sender and all intended recipients are located within the United States.” *Id.* § 1801(f)(3). Thus, for radio surveillance, when the NSA knows at least one party is outside the United States, FISA does not apply. In contrast, surveillance of wire communications falls within FISA if only one party is “in the United States” and if the surveillance itself “occurs within the United States.” *Id.* § 1801(f)(2). This summary omits a few details.

Executive Branch officials found this distinction untenable. Beginning at least in 2006, officials from the Intelligence Community and Justice Department pressed Congress repeatedly for a fix to FISA. Ken Wainstein, the Department of Justice's first Assistant Attorney General in charge of the National Security Division, suggested,

Rather than focusing, as FISA does today, on *how* a communication travels or *where* it is intercepted, we should define FISA's scope by reference to *who is the subject of the surveillance*. If the surveillance is directed at a person in the United States, FISA generally should apply; if the surveillance is directed at persons overseas, it shouldn't.²⁹

Former Director of National Intelligence, Admiral Michael McConnell, agreed, testifying that "[o]ur job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the Nation's security to a snapshot of outdated technology."³⁰

Congress eventually gave the Executive Branch what it wanted. First, in 2007, it enacted the PAA, which erased the wire and radio distinction for some cases, but out of concern for a rushed legislative process,³¹ it set a six-month sunset on the law.³² After the PAA expired, Congress enacted the FISA Amendments Act of 2008,³³ which took a different textual approach than the PAA, albeit to the same ends. As amended by the FISA Amendments Act, FISA no longer draws a distinction between communications carried by satellite and those carried by fiber-optic cables when non-U.S. persons are the target of the surveillance.³⁴ Now, intelligence analysts can listen to those communications no matter how they are carried—whether by copper wire, fiber-optic cable, microwave radio, satellite radio, or something else—under the same low standard. And because this part of FISA is now tech neutral, the same rules will apply to any communications technology developed in the future, regardless of how it operates, where it is deployed, or if it implicates privacy in new ways.

C. *The Arguments in Favor of Tech Neutrality*

This story of how and why Congress made FISA more neutral is typical. In many legislative debates over surveillance law, one side or another will

29. *Modernization of FISA*, *supra* note 27, at 30 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. of National Security, United States Department of Justice).

30. *Id.* at 19 (statement of J. Michael McConnell, Director of National Intelligence).

31. James Risen, *Bush Signs Law to Widen Reach for Wiretapping*, N.Y. TIMES, Aug. 6, 2007, at A1.

32. Protect America Act of 2007, Pub. L. No. 110-55, sec. 6(c), 121 Stat. 552, 557 (to be codified at 50 U.S.C. § 1803).

33. Pub. L. No. 110-261, 122 Stat. 2436 (to be codified in scattered sections of 50 U.S.C.).

34. *Id.* sec. 101, § 702. As amended, FISA now allows the Intelligence Community to monitor communications of non-U.S. persons not known to be in the United States, whether carried over wire or radio, without prior judicial approval, subject to some safeguards and checks, including mandatory notice to the FISA Court. *Id.*

urge Congress to reject tech specificity in favor of tech neutrality.³⁵ Those who argue for tech neutrality too rarely explain in detail the reasoning behind their arguments. Quite often, tech neutrality is a principle or rule, and it almost seems to go without saying.³⁶ Even when proponents of neutrality explain their reasoning, they often do so cursorily. As a result, we lack satisfying theoretical explanations for tech neutrality.³⁷ Before I offer counterarguments, I must first present the best arguments I can for tech neutrality in the surveillance context in order to try to avoid taking on straw men.

The arguments for neutrality are not inherently flawed, and sometimes tech neutrality may be a good idea. Still, these arguments are not unassailable, and they certainly do not support elevating the idea of tech neutrality to the level of a principle. Instead, they have gaps and logical flaws that suggest the shortcomings of the approach, which I will explore in Part II. These arguments number three.

1. *Consistency.*—The most often recited argument in favor of tech neutrality is the need for consistency—the need to avoid arbitrary distinctions between technologies that should be treated alike.³⁸ When Congress enacts a tech-specific rule, it regulates a specific technology while leaving unregulated similar technologies.³⁹ It makes no sense to treat these similar technologies differently because the policy rationale justifying the rule usually focuses on the effects of the technology, not on the function or features of the technology.⁴⁰

35. See *supra* notes 25–30 and accompanying text.

36. See, e.g., Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1127–28 (2009) (postulating that use limits are a better way to regulate border searches of laptops because special-collection limits would “violate the principle of technological neutrality”).

37. Some scholars have developed lists of explanations for tech neutrality. Chris Reed cites three aims: “futureproofing, online and offline equivalence, and encouraging the development and uptake of the regulated technology.” Reed, *supra* note 3, at 275. Similarly, Ilse van der Haar argues that tech neutrality leads to “non-discrimination, durability, efficiency, and certainty.” Corine Schouten, *EU Failed to Apply Technology Neutrality in Regulating Communication Services*, INNOVATIONS REP., Nov. 12, 2008, http://www.innovations-report.com/html/reports/communication_media/eu_failed_apply_technology_neutrality_regulating_124187.html. Almost all of these laudable qualities appear in the three arguments I present below.

38. See Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 299 (2009) (relating that the FISA Amendments Act “proceed[s] in a technology-neutral and less arbitrary fashion” than FISA).

39. See *Modernization of FISA*, *supra* note 27, at 10 (statement of J. Michael McConnell, Director of National Intelligence) (“FISA was written to distinguish between collection [of communications] on a wire and collection out of the air.”).

40. See *id.* at 28 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. of National Security, United States Department of Justice) (explaining that by embedding tech-specific language in FISA, Congress “use[d] the manner in which communications [were] transmitted as a proxy for the types of targets and communications that the statute intended to reach”); *id.* at 30 (arguing that instead of focusing upon “how a communication travels or where it is intercepted, [Congress] should define FISA’s scope by reference to *who is the subject of the surveillance*”).

Consistency sits at the heart of the Executive Branch arguments in favor of the PAA and FISA Amendments Act. Admiral McConnell, Assistant Attorney General Wainstein, and other Executive Branch officials repeatedly argued against treating satellite and fiber-optic communications differently.⁴¹ Consistency arguments often invoke happenstance and chance. Should the fact that a terrorist's communications happen to be carried over fiber-optic cable rather than via satellite have any bearing on whether the NSA can listen to them? Of course not, the tech-neutrality proponents argue.⁴²

2. *Keeping Up with Technological Change.*—Many argue that laws should be written neutrally because technology changes too quickly for the legislative process to keep up.⁴³ According to this argument, specificity leads inevitably and rapidly to anachronism because by the time a bill becomes a law, the technology will have evolved.⁴⁴ To support Admiral McConnell's call for tech neutrality in FISA, Andrew McCarthy of the *National Review* argued, "Any statute that focuses on technology will become obsolete (or worse, counterproductive) when technology changes . . ."⁴⁵ Those making particularly strong forms of this argument seem to hold tech neutrality up as a form of enlightened modernity; a recognition by Congress that something in society—technology—moves too quickly for the legislative process.⁴⁶ Outside the surveillance context, the Seventh Circuit explained, "[L]egislators . . . know that complexity is endemic in the modern world and that each passing year sees new

41. See *id.* at 13 (statement of J. Michael McConnell, Director of National Intelligence) ("FISA's definitions of 'electronic surveillance' should be amended so that it no longer matters how collection occurs (whether off a wire or from the air)."); *id.* at 34 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. of National Security, United States Department of Justice) ("In keeping with the preference for technological neutrality, we would eliminate the distinction between 'wire' and 'radio' communications that appears throughout [FISA].").

42. See *id.* at 11 (statement of J. Michael McConnell, Director of National Intelligence) ("Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the nation's security to a snapshot of outdated technology.").

43. See *id.* at 15 (advocating amendments that would "make FISA technology-neutral, so that as communications technology develops—which it absolutely will—the language of the statute does not become obsolete").

44. See, e.g., *id.* at 33 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. of National Security, United States Department of Justice) ("As a result of revolutions in communications technology since 1978, . . . the current definition of 'electronic surveillance' sweeps in surveillance activities that Congress actually intended to exclude from FISA's scope.").

45. Andrew C. McCarthy, *FISA Reform: The Bad Bill That Beats No Bill*, NAT'L REV. ONLINE, Feb. 14, 2008, <http://article.nationalreview.com/348094/fisa-reform-the-bad-bill-that-beats-no-bill/andrew-c-mccarthy?page=1>.

46. See *Modernization of FISA*, *supra* note 27, at 33 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. of National Security, United States Department of Justice) ("Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should this Congress. . . . We should not have to overhaul FISA each generation simply because technology has changed.").

developments. That's why they write general statutes rather than enacting a list of particular forbidden acts."⁴⁷

Furthermore, tech-specific laws do not simply become unacceptably anachronistic, but rather, they tend to become underinclusive with time. Once the specific type or class of technology targeted by a tech-specific law evolves into a new successor form, the law no longer applies. For those who support the policy underlying the law, this makes the law underinclusive, as they would prefer a law that expands to cover new versions of old technology.

Proponents of the PAA and FISA Amendments Act complained that the evolution of technology from satellite to fiber-optic cable communications had narrowed FISA.⁴⁸ According to their version of history, in 1978, when Congress enacted FISA, almost all transoceanic communications bounced through satellites using radio waves.⁴⁹

Times and technologies had changed. Thousands of miles of new fiber-optic cable had been laid since 1978, and the telecommunications industry had moved much of its operations from satellites to the new, cheaper, plentiful fiber-optic alternative.⁵⁰ By the time of the debates over the PAA, telephone companies were carrying most long-haul-phone calls over cables including, of course, the calls of terrorists and agents of foreign powers, creating an underinclusive, technological anachronism in the law.⁵¹ What Congress had chosen not to regulate in 1978, evolving technology had re-regulated.⁵²

The narrower FISA severely burdened the Intelligence Community. Admiral Michael McConnell argued, "Because technology has changed but the law has not, this statute—meant to protect against domestic abuses—instead protects potential foreign terrorists. We are significantly burdened in

47. *United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005).

48. See *infra* note 51 and accompanying text.

49. See *Modernization of FISA*, *supra* note 27, at 10 (statement of J. Michael McConnell, Director of National Intelligence) ("When the law was passed in 1978, almost all local calls were on a wire and almost all long-haul communications were in the air . . .").

50. See Declan McCullagh & Anne Broache, *NSA Eavesdropping: How It Might Work*, CNET NEWS, Feb. 7, 2006, http://news.cnet.com/NSA-eavesdropping-How-it-might-work/2100-1028_3-6035910.html?tag=mncol (explaining that today "an undersea web of fiber-optic cables spans the globe—and those carry the vast majority of voice and data that leave the United States" so that "99 percent of the world's long-distance communications travel through fiber links [and] the remaining 1 percent . . . are satellite-based").

51. See *Modernization of FISA*, *supra* note 27, at 10–11 (statement of J. Michael McConnell, Director of National Intelligence) (explaining that, in 1978, because most local calls were wire communications and most international calls were wireless communications, FISA's scope included wire communications; today, "the situation is completely reversed").

52. See *id.* at 19 (statement of Kenneth L. Wainstein, Assistant Att'y Gen. of National Security, United States Department of Justice) (explaining that technological "advances have largely upended FISA's intended carve-out of intelligence activities directed at persons overseas" so that "considerable resources of the Executive Branch and the FISA Court are now expended on obtaining court orders to monitor the communications of terrorist suspects overseas").

capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States.”⁵³ Similarly, Assistant Attorney General Wainstein testified that “sweeping changes since 1978—both in the nature of the threat that we face and in telecommunications technologies—have upset the delicate balance that Congress sought to achieve when it enacted FISA.”⁵⁴

3. *Institutional Competence.*—Finally, tech-neutral provisions respond to institutional concerns, helping Congress do what it does well and avoid doing what it does poorly. Those who argue against tech-specific statutes often intimate or assert that Congress is not equipped to understand complicated new technologies.⁵⁵ These arguments echo themes from each of the prior arguments—about consistency and the rate of technological change—tying them specifically to Congress’s perceived institutional shortcomings. As Bruce Berkowitz of the Hoover Institution puts it, “Intelligence officials know what they really require to do their mission, and legislators know how to write authorizing legislation.”⁵⁶ General Michael Hayden, then-Director of Central Intelligence, testifying about FISA, suggested that legislators were not equipped to keep up with changing technology: “Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should you. . . . [T]he statute we develop should be technology neutral.”⁵⁷

II. The Problems with Tech Neutrality

On the surface, these arguments have undeniable persuasive force, but they fare poorly under closer scrutiny. Every purported benefit of tech neutrality—consistency, avoidance of underinclusiveness, and institutional competence—can be recast as a shortcoming instead. These shortcomings are best illustrated through laws other than FISA, allowing us to draw lessons from older debates about the laws governing criminal surveillance. Consider the significant downsides of tech neutrality.

53. Mike McConnell, Letter to the Editor, *Protecting Americans and Their Rights*, N.Y. TIMES, May 5, 2007, at A12.

54. *Modernization of FISA*, *supra* note 27, at 24 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. of National Security, United States Department of Justice).

55. Often arguments like these carry a hint of superiority and maybe even a sense of ridicule. Perhaps other societal institutions can keep up with technology, but not Congress, which is stodgy and out of touch, full of elderly members who are the same. See, e.g., Jim Puzzanghera, *Weighing High-Tech Bills in Analog: Political Issues Pile Up in the Fast-Evolving Sector, but Congress’ Expertise Isn’t Up To Date*, L.A. TIMES, Aug. 7, 2006, at C1 (cataloging the frustration of business leaders in educating Congress on technology and noting the substantial ridicule heaped on former Senator Ted Stevens for describing the Internet as “a series of tubes”).

56. Bruce Berkowitz, *The Wiretap Flap Continues*, WALL ST. J., Sept. 18, 2007, at A15.

57. *FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 8 (2006) (statement of Michael V. Hayden, Director, Central Intelligence Agency).

A. *Treating Differences Alike*

While the law should not treat different technologies differently when doing so would reward happenstance and chance, it is also true that some differences deserve to be treated differently. If instead Congress, trying not to violate the “principle” of tech neutrality, treats such differences alike, it will produce ineffective laws with unpredictable or pernicious effects.

As many have written, in our modern, information-driven world, technology acts like architecture, constraining and enabling certain human behavior.⁵⁸ But because different technologies constrain to different degrees and in different ways,⁵⁹ we should not regulate any specific technology until we take the time to study it to allow us to tailor our laws and regulations to the idiosyncrasies of the specific context. Policy makers fail to do this when they enact tech-neutral laws.

Many information-privacy scholars have recognized this point, arguing that policy makers should respond to the diversity of technology by tailoring and differentiating regulation to the specific context. Helen Nissenbaum has argued that expectations of privacy turn entirely on deeply contextualized differences between situations.⁶⁰ Dan Solove has written extensively about how changing technology brings new challenges to privacy.⁶¹ In part because of the diversity of privacy-impacting technologies, he concludes that privacy cannot be described monolithically but instead should be considered as a complex of different values that relate to one another only through Wittgensteinian “family resemblances.”⁶²

Scholars writing about national security and criminal law have drawn similar conclusions. Orin Kerr has written extensively about how specific new forms of technology enable both new forms of surveillance and new methods for committing crime.⁶³ He argues that these differences matter to criminal procedure and suggests rules that take these subtle differences into account.⁶⁴ Similarly, Jack Balkin and Sandy Levinson write persuasively about how “new technologies of surveillance, data storage, and computation”

58. See, e.g., LAWRENCE LESSIG, *CODE: VERSION 2.0*, at 77–79 (2006) (arguing that the way in which any given technology is implemented—and selected from among the many potential architectures—is an exercise of power with political and social consequences).

59. See *id.* at 203–07 (cataloging the privacy consequences inherent in the specific architecture of several modern technologies).

60. HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* 2–3 (2009).

61. See, e.g., DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 9 (2004) (decrying the inadequacy of existing law protecting information privacy in response to the emergence of digital dossiers).

62. Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1090–91 (2002).

63. E.g., Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 864–67 (2004) (charting Fourth Amendment treatment of various technological developments).

64. See *id.* at 868–75 (contrasting the institutional competence of the Legislature and Judiciary in addressing the implications of new technology on these areas of law).

have contributed to the rise of what they call the “National Surveillance State,” characterized by a significant increase in the amount of intelligence and surveillance the government conducts in the name of protecting national security.⁶⁵

The message from the overwhelming weight of legal scholarship about technology, privacy, and national security recommends subtlety and nuance, yet when Congress embraces uncritically the principle of tech neutrality, it abandons subtlety and nuance in the name of consistency.

Consider the ongoing Fourth Amendment debate over the search of laptops at international borders. The Supreme Court has held that government agents at international borders can conduct a wide range of suspicionless searches without violating the Fourth Amendment because of the need to protect American sovereignty and because people crossing borders should and usually do expect less privacy.⁶⁶ Scholars have debated whether this rule should extend to files stored on laptops being carried across the border.⁶⁷

Civil liberties groups argue that laptops are special technologies that merit special treatment under the Fourth Amendment at the border.⁶⁸ Because laptops store vast amounts of information and because the information can be of a highly personal nature, laptops become extensions of the self, more akin to a home than a pad of paper in a traveler’s backpack.⁶⁹

Former Bush Justice Department official, now law professor, Nathan Sales disagrees, arguing that the “principle of technological neutrality” demands a rule that treats pads of paper and laptops consistently.⁷⁰ But Professor Sales errs if he means to invoke a freestanding principle of neutrality, one that must be “violated” only with good justification. The only principle Congress should invoke is this one: Treat similar technologies alike and differing technologies differently. Arguing that a technology is not sufficiently different to outweigh a principle of neutrality is to double count.

To be fair, Professor Sales relies not only on the principle of neutrality; he also compares the privacy risks from searches of laptops to searches of

65. Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 *FORDHAM L. REV.* 489, 520–22 (2006).

66. See *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) (“Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant Automotive travelers may be stopped at fixed checkpoints near the border without individualized suspicion even if the stop is based largely on ethnicity” (citations omitted)).

67. E.g., Symposium, *The Fourth Amendment at the International Border*, 78 *MISS. L.J.* 241 (2008).

68. Brief for Amici Curiae Ass’n of Corporate Travel Executives & Electronic Frontier Foundation in Support of Defendant-Appellee at 4, *United States v. Arnold*, 523 F.3d 941 (9th Cir. 2008) (No. 06-50581).

69. *Id.* at 11–12.

70. Sales, *supra* note 36, at 1115.

“letters, address books, photo albums, and similar items.”⁷¹ The comparison, however, should be the entire analysis; the invocation of a principle should add nothing.

B. *Technological Change*

Tech-neutral laws too often avoid the problem of underinclusiveness by permitting overinclusiveness. They expand to cover new technologies and new circumstances. Consider the Communications Assistance for Law Enforcement Act⁷² (CALEA), a law that requires telecommunications providers to design their systems to be readily wiretappable to accommodate lawful government requests for access to customer communications.⁷³ CALEA is a tech-neutral law, one directed at “telecommunications carrier[s]” that governs what they must do with “equipment, facilities, or services” that can be used by a customer to “originate, terminate, or direct communications.”⁷⁴

When CALEA was enacted in 1994, both the Justice Department, which pressed for the law, and Congress focused mostly on problems associated with digital telephone networks.⁷⁵ Although the Internet was growing in importance at the time, almost all of the attention in hearings and committee reports centered on how digital telephone switches were foiling lawfully authorized wiretaps.⁷⁶ Motivated by such a tech-specific fear, Congress could have written a tech-specific law, one focused on digital telephony or perhaps even one that cited particular protocols or products by name. Instead, Congress wrote a tech-neutral law.

As we should have anticipated, tech-neutral CALEA has expanded over time. In 2005, the Federal Communications Commission (FCC), using power delegated to it in CALEA, granted the Justice Department’s petition to apply CALEA to providers of broadband-Internet and interconnected-Voice-over-IP (VoIP) services.⁷⁷ The FCC came to this conclusion over the objections of privacy groups and affected service providers, most vocally groups representing libraries and universities that worried they would be required to

71. *Id.*

72. 47 U.S.C. §§ 1001–1021 (2006).

73. *Id.* § 1002(a).

74. *Id.* Under the law’s definitions, a “telecommunications carrier” is “a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire,” *id.* § 1001(8)(A), but excludes “information services,” *id.* § 1001(8)(C), those that “offer[] . . . a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications,” *id.* § 1001(6)(A).

75. See, e.g., H.R. REP. NO. 103-827, at 14 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3492 (calling on Congress to respond to the “‘digital telephony’ revolution”).

76. See *id.* at 10–16, *reprinted in* 1994 U.S.C.C.A.N. 3490–96 (summarizing the hearings on CALEA).

77. *In re Commc’ns Assistance for Law Enforcement Act and Broadband Access to Servs.*, 20 F.C.C.R. 14,989, 14,989 (2005).

include surveillance backdoors in their networks.⁷⁸ Ultimately, the D.C. Circuit rejected the challenges to the rulemaking.⁷⁹

Even one who agrees with this interpretation of the language of CALEA should concede that Congress did not say much about VoIP and broadband Internet when it considered whether to enact CALEA. When a tech-neutral law like CALEA expands over time, it loses its tether to the evidence Congress considered, the experts consulted in hearings, and the pages of research compiled into committee reports.

C. *Imprudent Delegation*

Of all of the arguments that support tech neutrality, the most important and the most flawed is the argument about institutional competence. Although Congress may sometimes have difficulty understanding the subtle nuances of technology or national security, a tech-neutral surveillance law rarely delegates Congressional power to an expert agency better equipped to understand such complexities. Instead, such a law almost always delegates power solely to the Executive Branch, which is often no better situated than Congress to understand such complexities.⁸⁰ When Congress switched from regulating “numbers dialed” to “dialing, routing, addressing, and signaling information,”⁸¹ it surrendered its role in future discussions about evolving technology because a tech-neutral law always expands with changing technology, placing the power entirely in the White House, NSA, and Justice Department.⁸²

D. *How to Decide Between Neutrality and Specificity*

Thus, every argument that supports the principle of tech neutrality can be met with a strong counterargument. We should never again treat legislative tech neutrality as a principle, default choice, or presumption; it is merely one of two paths we might take, and whether it is the right path depends on many circumstances. For example, to choose between tech neutrality and tech specificity, legislators need to understand how the technologies work, have been deployed, and have been used. Only by gathering accurate and

78. See, e.g., Final Brief for Petitioners at 43–44, *Am. Council on Educ. v. FCC*, 451 F.3d 226 (D.C. Cir. 2006) (No. 05-1404) (arguing, with libraries and universities among the petitioners, that the FCC’s interpretation would force private broadband providers to comply with surveillance-capability requirements).

79. See *Am. Council on Educ.*, 451 F.3d at 232–36 (rejecting petitioners’ claims that Internet broadband and VoIP services classify as “information services” under CALEA).

80. See *infra* subpart III(A).

81. See *supra* notes 11–12 and accompanying text.

82. See Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 76, 89 (2008) (discussing privacy-impact-assessment requirements that apply to new technology and privacy risks and also highlighting increased involvement by the White House in administrative action).

complete information about these topics, can legislators decide, for example, whether to treat two technologies alike or differently.

Unfortunately, in the debates surrounding the PAA and FISA Amendments Act, Congress might not have had accurate information about these critical circumstances, because according to some nongovernmental observers, Executive Branch officials had painted a misleading picture about the critical factual claim that “almost all transoceanic communications were [satellite] radio communications.”⁸³ This factual statement supported every single Executive Branch argument for making FISA tech neutral, thus serving as the foundation for Congress’s decision to expand the surveillance power under FISA.

At the time the Executive Branch was making this factual claim, Kate Martin and Lisa Graves of the Center for National Security Studies were rebutting it in congressional testimony:

[E]ven a general examination of telecommunications history reveals that the scenario [administration officials] posit claiming that virtually all international calls of Americans were via satellite radio and therefore intended to be obtained by the government is not accurate. While satellites were increasingly used in the 1970s for television broadcasting and some telecommunications, American telephone companies were continuing to rely on trans-oceanic cables for international calls, with newer transatlantic cables sunk even the year after FISA passed⁸⁴

The pair concluded, “A more accurate statement than the administration’s description would be that for [the] past 29 years, US telecommunications has relied on both wire and radio technology for domestic and international calls.”⁸⁵

These conclusions were corroborated by David Kris, writing at the time as a private citizen but now the Assistant Attorney General (AAG) for National Security in the Obama Administration. Mr. Kris rebutted the Administration’s claims about the evolution from satellite to wireline communications, finding them “exaggerated,” because “in and around 1978, transoceanic communications were made in relatively large quantities by *both* satellites (radio) *and* coaxial cables (wire); both kinds of systems were expected to continue in service for many years; and the use of fiber optics was already anticipated for undersea cables.”⁸⁶

83. *Modernization of FISA*, *supra* note 27, at 29 (statement of Kenneth L. Wainstein, Assistant Att’y Gen. of National Security, United States Department of Justice).

84. *Modernization of FISA*, *supra* note 27, at 195 (statement of Kate Martin, Director, and Lisa Graves, Deputy Director, Center for National Security Studies).

85. *Id.*

86. David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act 9* (Counterterrorism & Am. Statutory Law Series, Working Paper No. 1, 2007), available at http://www.brookings.edu/~media/Files/rc/papers/2007/1115_nationalsecurity_kris/1115_nationalsecurity_kris.pdf.

In other words, according to AAG Kris, the core factual premise underlying the Executive Branch's argument for tech neutrality might have been exaggerated. This might mean, as Ms. Martin and Ms. Graves argued and contrary to the Executive Branch's claims, that when Congress enacted FISA in 1978, it had good reason to treat radio and wireline communications differently.⁸⁷ Perhaps those reasons still merited inconsistent treatment in 2007 and 2008. My research has not yet confirmed which of the two versions of history should be believed. My point here is merely to suggest that one reason Congress might have failed to do a better job untangling these inconsistent histories is because it might have failed to see the importance of the inquiry, once it placed too much stock in the principle of tech neutrality.

III. The Argument for Tech-Specific Surveillance Laws

To this point, I have offered only arguments that challenge unchallenged claims for tech neutrality. There is no freestanding principle of tech neutrality, and arguments to shift from a specific to a neutral rule should be weighed on their own merits. But rejecting tech neutrality is not the same thing as defending tech specificity. Policy makers should take care not to make the same type of mistake in favor of tech specificity I have argued the proponents of tech neutrality have made; treating tech specificity as a freestanding principle is as bad as doing so with tech neutrality.

In this final Part, however, I will try to make that argument without making that mistake, giving reasons to often favor tech-specific laws over tech-neutral ones for surveillance. The most important reason was introduced in Part II: Tech-specific rules check the Executive Branch by authorizing narrow and circumscribed new forms of surveillance, permitting the Executive Branch the freedom to act with the Legislature's blessing, but only for a particular type of technology. We should prefer the active participation in surveillance decision making of two branches of government rather than one.

In order to embrace tech specificity, however, we need to deal with two practical difficulties, neither insurmountable. First, tech-specific laws expire as people switch from using the specified technology to using a replacement technology, leaving us adrift without legislative guidance. This would be unacceptable if it permitted either unchecked surveillance or untraceable crime or terrorism, but neither extreme is likely thanks to what I call the "background rules of surveillance."⁸⁸ Second, once law makers decide to create a tech-specific rule, they must decide how specific to make the rule, requiring a difficult textual balancing act.

87. See *Modernization of FISA*, *supra* note 27, at 195 (statement of Kate Martin, Director, and Lisa Graves, Deputy Director, Center for National Security Studies) ("[F]or [the] past 29 years, US telecommunications has relied on both wire and radio technology for domestic and international calls. From the beginning, FISA was written to accommodate that reality.").

88. See *infra* section III(B)(1).

Finally, tech-specific rules serve one unappreciated benefit: they sunset when new technologies are introduced. A law that governs only the use of a telephone, for example, will not govern the use of the Internet. Technology sunsets should be viewed as significant improvements over the traditional time-based sunsets that Congress seems to favor for surveillance laws lately. Technology sunsets enjoy many of the benefits and few of the downsides of their traditional counterparts. For all of these reasons, Congress should consider drafting tech-specific surveillance laws much more often than they have.

A. *Why We Should Prefer Specificity*

Sometimes Congress should delegate its authority to experts—to those with relative institutional advantages—but history has taught us to doubt that surveillance is a proper situation for delegation. The Executive Branch sees only one side to debates between security and privacy, and it tends to expand its authority and decrease oversight at every step. History has proven this repeatedly, from the well-documented wiretapping abuses at the FBI under J. Edgar Hoover,⁸⁹ to the intelligence abuses at the CIA that led to the Church Committee⁹⁰ and the enactment of FISA,⁹¹ to the NSA's Terrorist Surveillance Program,⁹² and to abuses of the national security letter process at the FBI.⁹³ The modern surveillance state needs information, and left without proper oversight, the analysts and agents in the field always seem to choose the path to more information and fewer administrative hurdles.⁹⁴ The Executive Branch, especially one bent on finding hidden terrorists, has shown that it cannot be trusted to act unchecked.⁹⁵

The Legislative Branch also brings another institutional advantage over the Executive Branch. The Executive Branch, especially the NSA, shrouds

89. See WHITFIELD DIFFIE & SUSAN LANDAU, *PRIVACY ON THE LINE* 163–64 (updated & expanded ed. 2007) (detailing the wiretapping of seventeen people for political purposes during the Nixon administration); Robert Bloom & William J. Dunn, *The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment*, 15 WM. & MARY BILL RTS. J. 147, 148–52 (2006) (comparing President Bush's warrantless wiretapping to Nixon's extensive wiretapping).

90. S. REP. NO. 94-755, at 24 (1976).

91. See S. REP. NO. 95-701, at 5 (1978), reprinted in 1978 U.S.C.C.A.N. 3973, 3973–74 (providing a history of FISA and attempting to “make more explicit the statutory intent, to provide further safeguards for individuals subjected to electronic surveillance”).

92. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

93. See Dan Eggen, *FBI Found to Misuse Security Letters*, WASH. POST, Mar. 14, 2008, at A3 (describing the FBI's use of national security letters to obtain personal data from U.S. citizens rather than foreigners).

94. See Kevin Poulsen, *FBI Seeks Internet Telephony Surveillance*, SECURITY FOCUS, Mar. 27, 2003, <http://www.securityfocus.com/news/3466> (detailing a request by the FBI and the Justice Department to require companies to make technical changes making eavesdropping easier).

95. See, e.g., Risen & Lichtblau, *supra* note 92 (detailing how President Bush allowed the United States to monitor phone calls without court intervention).

its entire operations in secrecy.⁹⁶ Although the Legislative Branch deals with national security matters through classified hearings, select committees, and security clearances, its members are all quintessentially public figures who probably think more about the public's interest than a typical, nameless Executive Branch analyst.

Thus, the Legislative Branch should not delegate away its checking power. But that is precisely what it does when it writes a tech-neutral surveillance law.

B. Implementation

Before we can embrace tech specificity wholeheartedly though, we need to address two important implementation challenges. First, tech-neutral laws have one clear advantage over tech-specific laws—longevity. A tech-specific law applies only so long as people use the specific technology, and when people shift to using other, newer technology, we are left with uncertainty. The good news is that surveillance tends to be governed by good enough background rules. Second, legislators drafting a tech-specific law will struggle to set the proper level of specificity, and below I set out some rules of thumb.

1. *Background Rules.*—Tech-specific laws, by definition, do not expand or shift with every advance in technology; instead they expire as technology progresses, sometimes quickly and sometimes gradually. The expiry of an important surveillance law may seem like catastrophe, deregulating both surveillance and privacy protection, permitting either undetectable crime and terrorism, unchecked surveillance, or worse, both. These worst-case scenarios should not worry us, however, once we recognize that surveillance and privacy tend to be protected by important background rules that step in to fill the void when statutes do not.

At the outset, note a seeming irony: background rules tend to be tech-neutral rules.⁹⁷ Background rules apply when tech-specific rules expire precisely because they are not tied narrowly to a particular technology. Thus, although this Article argues against tech-neutral statutes, it cannot dismiss tech neutrality entirely. Without tech-neutral background rules, we would not be able to enact tech-specific laws.⁹⁸

The most important source for background surveillance rules is the Fourth Amendment to the U.S. Constitution.⁹⁹ The Fourth Amendment sits

96. See JAMES BAMFORD, *THE PUZZLE PALACE* 357 (1983) (describing NSA's informal nickname, "No Such Agency").

97. See *infra* note 103 and accompanying text.

98. I thank Joe Feller for suggesting this point.

99. The Fourth Amendment provides,

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall

in the background because the Supreme Court interprets it in a generally tech-neutral manner, but this has not always been the case. Before *Katz v. United States*,¹⁰⁰ the Supreme Court construed the Fourth Amendment with tech specificity, for example, distinguishing between “spike mike” recording devices that intruded physically into the offices of the people being monitored and those that did not.¹⁰¹ The seeming hyperspecificity of this rule prompted the D.C. Circuit to note that it was “unwilling to believe that the respective rights are to be measured in fractions of inches.”¹⁰² Beginning with *Katz*, however, the Court has construed the Amendment more neutrally, asking whether new forms of surveillance invade a person’s “reasonable expectation of privacy.”¹⁰³

A neutral Fourth Amendment is necessary but not sufficient to serve as an appropriate tech-neutral background for tech-specific surveillance statutes. The Fourth Amendment must also avoid extreme conclusions—absolute prohibitions or permissions for new surveillance techniques. If the Fourth Amendment’s default background rule for surveillance were an absolute prohibition on the use of new surveillance technologies, then the Intelligence Community would lose access to information, and in the worst case, it would lose track of those trying to harm us. On the other hand, if the Fourth Amendment’s rule were absolute permission, meaning any unregulated surveillance technology could be used to its fullest extent with no possibility of review, then we would end up with far too many invasions of privacy than we are willing to tolerate. Either result would be unacceptable.

The good news is that the Fourth Amendment’s background rules for surveillance almost never sit at either extreme. Instead, the Fourth Amendment tends to operate somewhere in the middle, thanks to a feature of its jurisprudence that is never celebrated by scholars—its lack of clarity.

To quote the first line of Anthony Amsterdam’s seminal article, “For clarity and consistency, the law of the fourth amendment is not the Supreme

issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

100. 389 U.S. 347 (1967).

101. Compare *Goldman v. United States*, 316 U.S. 129, 133–34 (1942) (holding that the use of a spike mike that did not enter the apartment was not a search), with *Silverman v. United States*, 365 U.S. 505, 509 (1961) (holding that the use of a spike mike that made contact with an apartment baseboard was a search).

102. *Silverman v. United States*, 275 F.2d 173, 178 (D.C. Cir. 1960), *rev’d*, 365 U.S. 505 (1961).

103. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Despite the apparent neutrality of the reasonable-expectation-of-privacy test, the Court still seems to treat different technologies differently. See Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 307 (arguing that although *Katz* “was designed . . . to achieve some kind of technology neutrality within search and seizure law, . . . its impact on the law has been surprisingly narrow”).

Court's most successful product."¹⁰⁴ Other scholars have complained that "the Court has produced a series of inconsistent and bizarre results that it has left entirely undefended."¹⁰⁵ But for a background rule, inconsistency has a silver lining.

The muddiness of the Supreme Court's rule causes intelligence agents (and even more so their lawyers) to hesitate before charging ahead. As Carol Rose has said in praising muddy rules in property law, "When a court introduces ambiguity into the fixed rules that the parties initially adopted, it in effect reinstates the kind of weighing, balancing, and reconsidering that the parties might have undertaken if they had been in some longer term relationship with each other."¹⁰⁶ Because of the Fourth Amendment's muddiness, rarely should a government lawyer, pressed to analyze some new surveillance technology, tell an agent that he or she should proceed without worrying about the law.

Specifically, the Supreme Court and the federal courts of appeals have left unanswered two Fourth Amendment questions that arise in many contemporary surveillance situations: How does the Fourth Amendment apply to the Internet, and how does the Fourth Amendment apply to national security investigations involving foreign persons? We have only partial answers to these questions. *Smith v. Maryland*¹⁰⁷ stands for the proposition that government surveillance of some of the noncontent characteristics of electronic communication (specifically, the numbers dialed on a telephone) are not protected by the Fourth Amendment.¹⁰⁸ *United States v. District Court (Keith)*¹⁰⁹ stands for the proposition that the Fourth Amendment applies to national security investigations of domestic persons.¹¹⁰ These cases leave many important questions unanswered: Are the websites visited in a Web browser like the numbers dialed on a telephone and thus unprotected under *Smith*? Can *Keith* be extended to cover investigations of foreign persons? These are important questions that the Court should answer.

But recognize how the confusion over the Fourth Amendment plays a salutary role in the face of technological uncertainty. *Smith* provides a cautious green light to some aggressive new forms of surveillance, and *Keith* puts up at least a yellow light about national security investigations. The cases give government lawyers hope that they might be able to permit what their agents want to do without legislation, especially when the facts are important enough, but prevent them from charging forward without imposing

104. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 349 (1973).

105. Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 29 (1988).

106. Carol M. Rose, *Crystals and Mud in Property Law*, 40 STAN. L. REV. 577, 608-09 (1988).

107. 442 U.S. 735 (1979).

108. *Id.* at 742.

109. 407 U.S. 297 (1972).

110. *Id.* at 316-17.

some limits and controls on agents, as a hedge against future, adverse interpretations of the Fourth Amendment.

I have made two descriptive claims about the Fourth Amendment: After *Katz*, Fourth Amendment rules tend to be tech neutral, and the neutrality of these rules acts as a safety net, giving Congress the freedom to pass tech-specific statutes without worrying too much about what happens when the technology changes. But, turning to the normative, should the Fourth Amendment's rules be tech neutral, in light of the arguments against tech-neutral statutes in Part II? If so, then why might we value tech neutrality in our Constitution but reject it for statutes?

This normative question allows me to wade a bit into an illuminating debate that occurred between Professors Orin Kerr and Daniel Solove.¹¹¹ Although the pair disagreed about many things, they started from a point of fundamental agreement: both Congress and the courts play important roles in developing the rules of criminal procedure—Congress by passing the kind of surveillance statutes discussed throughout the instant Article, and the courts as interpreters of the Fourth Amendment.¹¹² Solove referred to this as a “dualist system of criminal procedure.”¹¹³

The pair disagreed, however, about which branch we should trust more to come up with good rules for criminal procedure, especially those designed to respond to new technology. Kerr argued that the Legislature has comparative institutional advantages over the courts for this task,¹¹⁴ while Solove wanted courts to play a more aggressive role than they had in the past.¹¹⁵ Rather than take a side in this debate, I argue that it is good to have *both* branches creating rules of criminal procedure. If nothing else, given institutional differences between the branches, they are likely to come to different conclusions about some surveillance practices, giving us more than one take on a subject, allowing us to use the different branches as laboratories to play out different ideas. Best of all, these approaches can support one another, each doing what the other does not. While the Constitution might serve as the wellspring of principle and baseline values, the statutes can fill in the details, policing the specifics of privacy and security. As Professor Kerr

111. The back-and-forth took place in three law review articles. Kerr, *supra* note 63; Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 *FORDHAM L. REV.* 747 (2005); Orin S. Kerr, *Congress, the Courts, and New Technologies: A Response to Professor Solove*, 74 *FORDHAM L. REV.* 779 (2005) [hereinafter Kerr, *Response*].

112. See Kerr, *supra* note 63, at 855 (“A broader look at the legal standards that govern criminal investigations involving new technologies suggests that Congress has often taken the lead, and . . . decisions interpreting the Fourth Amendment generally have played a secondary role. In some instances, congressional action has followed Supreme Court decisions interpreting the Fourth Amendment.”); Solove, *supra* note 111, at 753 (“The rules regulating government investigations have increasingly been those of federal statutes, not Fourth Amendment law.”).

113. Solove, *supra* note 111, at 747.

114. Kerr, *supra* note 63, at 858.

115. Solove, *supra* note 111, at 777.

noted, “[W]e should not expect the Fourth Amendment alone to provide adequate protections against invasions of privacy made possible by law enforcement use of new technologies. . . . Congress will likely remain the primary source of privacy protections in new technologies thanks to institutional advantages of legislatures.”¹¹⁶ At the same time, when tech-specific statutes, with their focus on detail and specifics, fail to apply because of changes in technology, the Constitution’s principles will provide the bulwark.

But even the advantages of interbranch diversity fail to explain fully why tech neutrality is so often a bad thing for Congress but not for the courts. This answer lies in one important institutional difference between the branches: courts adjudicate on a case-by-case basis, while legislatures design rules of general applicability.¹¹⁷ Given this difference, the amount of harm caused by a bad rule is much higher for legislative rules than judicial rules. When a legislature misreads the effect on privacy or security of a new technology or makes a bad prediction about the evolution of a future technology, the flawed general rule it creates as a result will apply broadly and will be hard to reverse. After enacting the rule, Congress will likely pay less attention to the question, making it hard for it to detect the effects of the bad rule. Further, in order to reverse the bad rule, Congress will need to muster the political will it needs to pass an amendment or repeal.

In contrast, when a judge crafts a rule based on a misreading of technology, it directly impacts only the parties in one case. In subsequent cases, judges applying the bad rule will have an opportunity to see how it applies to a new set of facts, which might expose the rule’s flaw. Law enforcement agencies or criminal defendants who disagree with the rule will have both the incentive and the opportunity in later cases to point out problems and to argue why the rule should be narrowed or reversed.

In addition to the Fourth Amendment, a second set of “rules” similarly sits somewhere between prohibition and permission, although it might seem odd to call these rules. They flow from the increasing intermediation of communications networks. In the early twentieth century, telephone and telegraph networks carried communications in the form of simple, easily captured analog signals, and surveillance targets tended to communicate from fixed locations like stationary landline telephones.¹¹⁸ On such simple analog networks, the government could conduct surveillance often without the help of an intermediary, for example attaching alligator clips to a wire

116. Kerr, *supra* note 63, at 838.

117. *Id.* at 884.

118. See K. A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance*, N.Y.U. REV. L. & SECURITY, 7 SUPP. BULL. ON L. & SECURITY, Spring 2006, at 3, available at <http://ssrn.com/abstract=889120> (“When FISA was being drafted it made sense to speak exclusively about the interception of a targeted communication—one in which there were usually two known ends and a dedicated (‘circuit-based’) communication that could be ‘tapped.’”).

atop a telephone pole or in an office building's basement.¹¹⁹ Things are much more complicated today. Digital packets have replaced analog signals, surveillance targets can access their e-mail accounts or use their cell phones from any place, and intermediaries can track communications that would have been untrackable before.¹²⁰

Now that the government needs help from private parties to conduct new forms of surveillance,¹²¹ a second background rule operates. Large corporate telecommunications providers worry about being sued by their customers for assisting the government. They worry especially about requests for novel forms of surveillance that may be inconsistent with specific congressional authority or at least unaccompanied by judicial order.¹²² Sometimes, providers overcome this reluctance, as when telephone and Internet providers complied with Bush Administration requests for assistance following 9/11.¹²³ Despite the pressure to cooperate with such requests, however, some providers have resisted government requests that they have felt might contradict the law.¹²⁴ Like the Fourth Amendment's muddy rules, intermediary risk aversion and exposure to liability leads to moderation. Nervous intermediaries will resist overly aggressive, broadly worded, or incompletely authorized new forms of surveillance, but they will also bend to the will of law enforcement and the Intelligence Community when a case seems important or urgent enough, as in the days following 9/11.

Both of these sets of background rules, Fourth Amendment rules and intermediary conservatism, help prevent the worst scenarios after a tech-

119. See *Olmstead v. United States*, 277 U.S. 438, 456–57 (1928) (describing the government's means of wiretapping as inserting small wires along ordinary telephone wires).

120. See Taipale, *supra* note 118, at 1 (describing FISA's inadequacy in addressing new technological developments).

121. Kenneth R. Logsdon, Note, *Who Knows You Are Reading This? United States' Domestic Electronic Surveillance in a Post-9/11 World*, 2008 U. ILL. J.L. TECH. & POL'Y 409, 419 (discussing the government's use of the private telecommunications industry in a new surveillance program).

122. See H.R. REP. NO. 99-690, at 15–16 (1986), *reprinted in* 1986 U.S.C.C.A.N. 5327, 5341–42 (noting that private parties are concerned with issues of liability when cooperating with FBI investigations); Albert Gidari, Jr., Keynote Address at the University of San Francisco Law Review Symposium: Companies Caught in the Middle (Oct. 28, 2006), *in* 41 U.S.F. L. REV. 535, 546–47 (2007) (describing cell-phone providers resisting requests for location-tracking information).

123. See Gidari, *supra* note 122, at 541 (“September 11 . . . changed a lot of things for service providers.”); Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, available at http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm (asserting that AT&T, Verizon, and Bellsouth all furnished the NSA with customer records after 9/11); Risen & Lichtblau, *supra* note 92 (describing a massive, warrantless monitoring effort made on thousands of international phone calls and e-mails from people inside the United States).

124. See Cauley, *supra* note 123 (“Among the big telecommunications companies, only Qwest has refused to help the NSA Qwest declined to participate because it was uneasy about the legal implications of handing over customer information to the government without warrants.”); Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, Jan. 20, 2006, at A1 (describing Google's refusal to comply with a broad subpoena for copies of its search-query records); Declan McCullagh, *DOJ Abandons Warrantless Attempt to Read Yahoo E-mail*, CNET NEWS, Apr. 16, 2010, http://news.cnet.com/8301-13578_3-20002722-38.html (describing Yahoo's refusal to comply with a court order for evidence in a criminal investigation).

specific rule lapses—unchecked permission or absolute prohibition. The background rules, therefore, should give Congress the reassurances it needs to build narrowly crafted tech-specific rules without worrying about chaos after the new law expires. At the same time, because the Fourth Amendment and intermediary cautiousness lead inherently to doubt and conservatism, these rules must usually stay in the background only, and Congress should eventually regulate to replace laws that expire.

2. *How Specific?*—After identifying and weighing background rules, if Congress chooses to enact a tech-specific law, it next needs to describe the technology at the proper level of specificity. Congress should strive to write statutes that talk about technology specifically enough to allow for the benefits of tech specificity but generally enough to prevent the need to revisit the statute every six months.

Striking the balance between breadth and specificity can be difficult. To start, Congress should look at the specific technology or technologies that motivated it to act. Perhaps a news story or anecdote about a specific type of surveillance technology brought the issue to Congress's attention. For example, consider the barrage of media attention paid in late summer, 2000, to Carnivore.¹²⁵ Carnivore was the name given by the FBI to a packet-sniffing-and-filtering device that could be used to track Internet behavior.¹²⁶ Although the tool was originally vilified in the press and by privacy groups,¹²⁷ with the benefit of time, this criticism seems a bit mistargeted. According to several scholars, the tool was used only with a court order and only when an Internet Service Provider (ISP) lacked the expertise to conduct the ordered surveillance itself.¹²⁸

Nevertheless, in 2000, Congress expressed concern and outrage over Carnivore. Within weeks of the first news reports, Congress held hearings in which members criticized Justice Department and FBI officials for having

125. See, e.g., Neil King Jr. & Ted Bridis, *FBI's Wiretaps to Scan E-mail Spark Concern*, WALL ST. J., July 11, 2000, at A3 (describing how Carnivore is “[e]ssentially a personal computer stuffed with specialized software [and] represents a new twist in the federal government’s fight to sustain its snooping powers in the Internet Age”).

126. See Trenton C. Haas, Note, *Carnivore and the Fourth Amendment*, 34 CONN. L. REV. 261, 271–73 (2001) (providing a detailed description of Carnivore).

127. See, e.g., Ted Bridis & Neil King Jr., *Carnivore E-mail Tool Won't Eat Up Privacy, Says FBI*, WALL ST. J., July 20, 2000, at A28 (discussing concerns about invading the privacy of Americans not under investigation for crimes).

128. See, e.g., Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1445 (2004) (describing Carnivore as a “tool the FBI developed to overcome difficulties service providers had in isolating and delivering the contents of electronic communications or addressing or routing information in response to court orders”); Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 653 (2003) (noting that, at times, “ISPs lack the expertise or the willingness to implement court orders on law enforcement’s behalf”).

developed the device.¹²⁹ Congress turned this criticism and concern into legislation, including in the USA PATRIOT Act a little-discussed provision specifically targeting Carnivore and similar tools. Section 216 of the Act obligates law enforcement to file a sealed report with a court when it uses tools like Carnivore.¹³⁰ Congress did not refer to Carnivore by name, choosing instead to refer to any “pen register or trap and trace device on a packet-switched data network.”¹³¹

This law seems appropriately tech specific, but consider other paths Congress might have taken. One year after the USA PATRIOT Act, with lingering fears about Carnivore on its mind, Congress passed another new reporting law, one which required much more detailed reporting while at the same time being much more narrowly defined.¹³² In this new law, Congress referred specifically to the name and model number given to Carnivore after the publicity fiasco, DCS-1000.¹³³ This law required the Attorney General to provide detailed reports about “the use of the DCS 1000 program (or any subsequent version of such program)” for two years.¹³⁴

Congress made a mistake drafting such a specific provision. Surveillance laws should not refer to specific tools by model and version number, even with the caveat applying the law to “any subsequent version.” While this type of hyperspecificity might make sense for the expert pronouncements of an administrative agency, Congress itself should rarely, if ever, refer to technology by a specific model number.

But this lesson in overspecificity provides a road map for finding the right level of generality. For any technology, one can recite a series of descriptions of increasing generality.¹³⁵ In the case of Carnivore, we progress from the most specific—DCS-1000—all the way to the most general—surveillance software or, even more generally, software.¹³⁶ Congress should avoid both extremes, the former being too specific, the latter too neutral by its generality. One possible target is to describe the technology at one or two steps above the most specific level. In this case, perhaps the ideal level of

129. See, e.g., *Fourth Amendment Issues Raised by the FBI's "Carnivore" Program: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. 107 (2000) (statement of Rep. Bob Barr, Member, H. Comm. on the Judiciary) (noting that the impact of Carnivore on the privacy rights of U.S. citizens is “immense”).

130. USA PATRIOT Act of 2001, Pub. L. No. 107-56, sec. 216, 115 Stat. 272, 289 (codified at 18 U.S.C. § 3123(a)(3)(A) (2006)).

131. *Id.*

132. 21st Century Department of Justice Appropriations Authorization Act, Pub. L. No. 107-273, 116 Stat. 1758 (2002) (to be codified in scattered titles of U.S.C.).

133. *Id.* sec. 305.

134. *Id.*

135. Copyright law embraces a similar “abstractions test,” first recited by Judge Learned Hand. *Nichols v. Universal Pictures Corp.*, 45 F.2d 119, 121 (2d Cir. 1930).

136. See Kerr, *supra* note 128, at 653–54 (discussing Carnivore and “its progeny” the “DCS-1000” in comparison to other software).

abstraction would be “packet-capture device” or maybe “filtered-packet-capture device.”

Although the standard outlined in this section is necessarily vague, it may prove easy to apply. Consider a few other surveillance technologies that in recent years have sparked the public’s imagination: In order to regulate these technologies, Congress should target “keystroke logging software” but never “Magic Lantern” (too specific) nor “spyware” (too general);¹³⁷ regulate “heat sensing cameras” rather than the “Agema Thermovision 210” or cameras;¹³⁸ and “whole-body scanners” instead of “L-3 Provision” or “radiation scanners.”¹³⁹

C. *Technological Sunsets*

Because tech-specific laws expire when technology changes, we can think of them as alternatives to traditional sunset provisions—legislative enactments that expire after a set period of time. In the surveillance context, Congress has enacted a number of sunset provisions in the past decade.¹⁴⁰ Tech-specific laws and laws with sunsets have much in common. Jacob Gersen, who has written frequently about sunset provisions,¹⁴¹ gives three reasons legislators enact sunset provisions: to offset information asymmetries, reduce error costs in the face of uncertainty, and correct limits of cognitive bias.¹⁴² Tech-specific provisions can also satisfy these three roles, by helping offset the doubt and uncertainty legislators have about the evolution of technology.

For example, imagine that a legislative proposal authorizing a new form of surveillance has a little less than a majority of Congress in support and a vocal contingent fiercely opposed. To help muster the few more votes they need, proponents of the bill might offer a traditional time-limited sunset provision, expiring say in four years. This serves two purposes: it helps

137. See Ted Bridis, *FBI Develops Eavesdropping Tools*, WASH. POST, Nov. 22, 2001, at A15 (describing the FBI’s “Magic Lantern” technology that “would allow investigators to secretly install over the Internet powerful eavesdropping software that records every keystroke on a person’s computer”).

138. See *Kyllo v. United States*, 533 U.S. 27, 29 (2001) (discussing whether the use of an “Agema Thermovision 210” thermal imager to detect infrared radiation emitting from Kyllo’s home constituted a Fourth Amendment search).

139. See Schwartz, *supra* note 4 (debating the use of screening technologies that can show the contours of the body and reveal foreign objects in reference to risks of privacy invasion).

140. See, e.g., Protect America Act of 2007, Pub. L. No. 110-55, sec. 6(c), 121 Stat. 552, 557 (to be codified at 50 U.S.C. § 1803) (setting a 180-day sunset on select provisions of the Act).

141. See, e.g., Jacob E. Gersen, *Temporary Legislation*, 74 U. CHI. L. REV. 247 (2007) (analyzing the “historical, legal, and political implications of temporary legislation”); Jacob E. Gersen & Anne Joseph O’Connell, *Deadlines in Administrative Law*, 156 U. PA. L. REV. 923 (2008) (discussing the use of deadlines to control the timing of administrative agency actions); Jacob E. Gersen & Eric A. Posner, *Timing Rules and Legal Institutions*, 121 HARV. L. REV. 543 (2007) (investigating constitutional, statutory, and internal congressional rules that affect the timing of legislative and executive actions).

142. Gersen, *supra* note 141, at 248.

convince undecided members to support the bill, by guaranteeing them a second vote in the near future, and it dampens the intensity of the opposition, who might fight less forcefully if they are guaranteed a future opportunity to kill the law. But the bill's proponents should recognize another way they might save the bill, by changing tech-neutral provisions into tech-specific provisions. If undecided and opposition law makers recognize that a tech-specific provision also expires at some point in the future, they may treat it the way they treat a traditional sunset.

More importantly, tech-specific laws overcome a significant limitation of ordinary sunsets. By "expiring" not according to an arbitrary timetable but instead precisely when changes in technology give reason to reopen policy debates, tech-specific laws offer the benefits of sunset without some of the downsides. To understand the relative advantages of technology sunsets, we need to understand some of the more technical details of Gersen's model as well as some of the model's shortcomings.

Gersen uses a transactions costs-public choice model to compare sunset legislation to permanent legislation.¹⁴³ Legislators must expend "enactment costs" when they enact or, in the case of a "sunsetting" law, reenact legislation, and they must expend "maintenance costs" at all other times.¹⁴⁴ For example, finding enough votes for passage is an enactment cost, while beating back an effort to repeal a law after it has been enacted is a maintenance cost.¹⁴⁵

As Gersen himself concedes, this model, although clarifying, proves difficult to apply because so much depends on unpredictable circumstances. How high are enactment costs versus maintenance costs? How much do legislators discount future enactment costs? Doubts about the answers to questions like these prevent Gersen from coming to many categorical conclusions about the differences between temporary and permanent legislation,¹⁴⁶ and they probably leave legislators making crude guesses about the effect of using a sunset or the amount of time to give to a sunset period.

Think of these difficulties as the products of a simple calibration problem. If a sunset period is set too far in the future, then the law may persist after the time when legislators would have otherwise wanted to revisit or even repeal the law. Even worse, if the sunset period is set to expire too soon, legislators will be forced to expend the costs of reenactment, even when there is no need for further review or debate. For any piece of

143. *Id.* at 261–66.

144. *Id.* at 263–65.

145. *Id.*

146. *See id.* at 266 ("While the analysis does not demonstrate that temporary legislation is clearly less costly than permanent legislation, it does show that temporary legislation is not clearly inferior—at least along the transaction-cost dimension."). Gersen comes to some tentative conclusions, for example arguing that "[i]t is almost certainly easier to block the repeal of legislation than to pass new legislation. As a result, continuing permanent legislation is less costly in the sunset year than reauthorizing temporary legislation." *Id.* at 264–65.

traditionally sunseting legislation, there is an ideal but unknowable term of expiration. The reason the ideal term cannot be known is because of the difficulty predicting the rate of change of important facts, particularly when those facts involve evolving technology.

Thinking of this as a calibration problem illuminates why tech-specific laws are better. A well-written tech-specific law is calibrated to expire precisely when the most important facts have changed enough to justify a reevaluation. As an example, consider how the technological shift from the telephone to the Internet expired an old version of the Pen Register Act at an optimal time.

The Pen Register Act regulates the government's ability to monitor the so-called envelope information associated with electronic communications.¹⁴⁷ For example, pen-register orders are needed to observe the numbers dialed by a telephone user.¹⁴⁸ Before the USA PATRIOT Act amended the Pen Register Act, it referred only to "numbers dialed,"¹⁴⁹ which meant it could expand without congressional reauthorization, but only to a point. As the telephony state of the art shifted from landline phones to cordless phones to mobile phones, the Pen Register Act expanded to cover each change, without wasteful congressional intervention.¹⁵⁰ This seems appropriate: although the surveillance of a mobile phone raises some issues not raised by the surveillance of a landline telephone, the two technologies seem similar enough to obviate the need for new congressional deliberation. The tech-specific law avoids the problem of laws tuned to expire too soon.

But then, people began to communicate over the Internet. Surely "numbers dialed" did not cover Internet-envelope surveillance, meaning Congress had to reconsider envelope surveillance as more people began to embrace this revolutionary new technology. The old technological sunset had expired. This seems well calibrated. Seen through both the privacy and law enforcement lenses, monitoring envelope information on the Internet seems a difference in kind not merely in degree from telephone surveillance. Precisely when the promise and peril of the Internet came into view, Congress was thrust back into the conversation. To be sure, great transaction costs were incurred—the first few times the Justice Department asked for changes to the Pen Register Act, Congress refused, partly because privacy advocates pushed back—but after it had time to deliberate fully, and once

147. 18 U.S.C. §§ 3121–3127 (2006).

148. *Id.* § 3121(a).

149. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, sec. 301, § 3126(3), 100 Stat. 1848, 1871.

150. *Cf. In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 749, 752–53 (S.D. Tex. 2005) (permitting the use of a pen register to obtain information from a mobile phone).

spurred by 9/11, Congress granted the new authority as part of the USA PATRIOT Act.¹⁵¹

Imagine how much less efficient it would have been for Congress to reevaluate the Pen Register Act on a fixed timetable, no matter what length of time it chose. If Congress had set the Pen Register Act to expire after four years, then at the end of the first term in 1990, there would have been very little to discuss. Communications did not change much in that time period. Congress would have been forced to expend resources to reenact the bill, perhaps placing it back under another four-year term, and it probably would have faced pressure after the first term to switch to a permanent term instead. The opposite problem might have occurred had the original sunset been set too far in the future, say ten years. In 1996, at the end of the first term, the Internet explosion would have been still in its infancy, and it might have been too soon to discuss an amendment. Then, if Congress had reenacted the Act with a second ten-year term, it is doubtful that it could have waited until the second date of expiry, in 2006, to finally get around to extending the Act to the Internet. Instead, the technological sunset forced a reevaluation at what seems to have been a near-optimal time: five years after Americans began to adopt the Internet in large numbers.¹⁵²

Conclusion

Conventional wisdom suggests that Congress should write tech-neutral surveillance laws most of the time. The conventional wisdom has it backwards. Congress should narrowly target surveillance laws at specific technologies most of the time. By doing so, it can assert its oversight role over the Executive Branch, which too often abuses its surveillance power when it acts unchecked, and shine a light on surveillance abuses.

151. See Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1194–95 (2004) (explaining how the amendments to the Pen Register Act mirrored those “the Justice Department had suggested for several years” before 9/11).

152. See U.S. CENSUS BUREAU, *COMPUTER AND INTERNET USE IN THE UNITED STATES: 2003* (2005), <http://www.census.gov/prod/2005pubs/p23-208.pdf> (reporting that between the years 1997 and 2000, the percentage of American households with Internet use at home rose from 18% to 41.5%).

The Law of Homegrown (Counter)Terrorism

Samuel J. Rascoff*

On the eve of World War II, concern mounted within the Federal Bureau of Investigation (FBI) that domestic intelligence related to national security was being gathered by local police, especially by members of major metropolitan police departments, and that the police were refusing to share the information they obtained with federal authorities.¹ FBI Director J. Edgar Hoover lobbied Attorney General Frank Murphy who, in turn, engaged the President.² On September 6, 1939, FDR issued the following directive: “The attorney general has been requested by me to instruct the Federal Bureau of Investigation of the Department of Justice to take charge of investigative work in matters relating to espionage, sabotage, and violations of the neutrality regulations.”³ It went on to urge “all police officers, sheriffs, and all other law enforcement officers in the United States promptly to turn over to the nearest representative of the Federal Bureau of Investigation any information obtained by them relating to espionage, counterespionage, sabotage, subversive activities and violations of the neutrality law.”⁴

This short vignette serves as a powerful reminder that local officials and agencies have historically participated in urgent matters of national security—especially in what we would today label “intelligence”—and in

* Assistant Professor of Law, New York University School of Law. Director of Intelligence Analysis, New York City Police Department (2006–2008). Thanks to members of the NYU School of Law Faculty Workshop, the Hoover Task Force on National Security, and the Texas Law Review Symposium for helpful comments. Thanks especially to Jennifer Arlen, Rachel Barkow, Philip Bobbitt, Bobby Chesney, Nick Colten, Adam Cox, Noah Feldman, Jack Goldsmith, David Golove, Karen Greenberg, Rick Hills, Stephen Holmes, Jim Jacobs, Rick Pildes, Ricky Revesz, Stephen Schulhofer, Jerry Skolnick, Dick Stewart, Matt Waxman, Rebecca Weiner, and Kenji Yoshino for beneficial suggestions. Superb research assistance was furnished by Charles Gussow and Jason Porta. The staff of the Texas Law Review edited with care and insight.

1. See 1 NAT'L COUNTERINTELLIGENCE CTR., A COUNTERINTELLIGENCE READER: AMERICAN REVOLUTION TO WORLD WAR II 171 (Frank J. Rafalko ed., 2004) [hereinafter CT READER] (describing the creation of the New York City Police Department's (NYPD) “special sabotage squad,” which resulted in citizens giving information regarding espionage to the local police rather than the FBI).

2. *Id.* at 169–70.

3. *Id.* at 177.

4. *Id.* The commandeering logic behind the directive would nowadays, in all likelihood, run afoul of the doctrine established in *Printz v. United States*, 521 U.S. 898, 935 (1997), which held that state police officials could not be involuntarily required to assist in the enforcement of a federal regulatory regime. But see *Dole v. South Dakota*, 483 U.S. 203, 211–12 (1987) (permitting the federal government to avoid state-sovereignty limitations on commandeering by making the receipt of federal funds conditional on state cooperation).

doing so have frequently rankled their federal counterparts.⁵ Before the rise of the Cold War bureaucracy effectively made national security synonymous with security furnished at the federal level,⁶ local police departments fielded intelligence units and carried out significant national-security-related missions.⁷

With the contemporary counterterrorism agenda giving impetus to discussions of (and practical developments in) domestic intelligence, local police have once again emerged as a significant constituency in discussions of national security.⁸ This is especially true in view of the ascendancy of homegrown terrorism,⁹ the phenomenon whereby individuals and groups

5. See BEVERLY GAGE, *THE DAY WALL STREET EXPLODED 173* (2009) (recounting how the NYPD was actively involved in the investigation of the September 16, 1920 Wall Street bombing); Adam M. Giuliano, *Emergency Federalism: Calling on the States in Perilous Times*, 40 U. MICH. J.L. REFORM 341, 362 (2007) (“The Framers incorporated limited but significant state roles regarding national defense and homeland security.”).

6. It was precisely the distinctive structural features of the Cold War and the bipolar nuclear conflict that it ushered in that caused the role of locals in national security to recede from view. See Ian Anderson et al., *Assessing the Terrorist Threat to America*, NAT’L ASS’N COUNTY ADMINS., http://www.countyadministrators.org/index.asp?Type=B_BASIC&SEC={EA2CBDBC-E2FD-4C32-AC04-D0430ACB34A2}&DE={83EACB65-3B6B-419F-9613-580ADCF39A5E} (“The Cold War, with its theories such as deterrence and mutual assured destruction, dominated national security A centralized and hierarchical enemy demanded the same to combat it.”).

7. The historical record of local involvement in domestic intelligence, no different from federal, is decidedly mixed. As Morgan has observed, in Chicago, the police department’s intelligence unit—a true “red squad”—became very closely linked with Mayor Daley and concerned itself with spying on his political opponents. RICHARD E. MORGAN, *DOMESTIC INTELLIGENCE* 84 (1980). The NYPD’s Bureau of Special Services and Intelligence (BOSSI) enjoyed a different reputation. *Id.* “BOSSI did not respond to City Hall concerns about political opponents and prided itself on its independence.” *Id.* at 85. Unlike Chicago, “the New York operation focused on the law enforcement utility of the information it gathered.” *Id.* Mayor Lindsay and Police Commissioner Murphy (well-known as a progressive) disbanded BOSSI in the mid-1960s and replaced it with the Intelligence Division, as it is still known. *Id.* Allegations of illegal activities made against the Intelligence Division beginning in the 1970s culminated in a consent decree that continues to bind the NYPD. See *Handschu v. Special Servs. Div.*, 605 F. Supp. 1384, 1417 (S.D.N.Y. 1985) (approving a consent decree that governs investigation and surveillance of political-action groups by the NYPD). See generally Paul G. Chevigny, *Politics and Law in the Control of Local Surveillance*, 69 CORNELL L. REV. 735, 751–67 (1984) (discussing the circumstances leading up to and the specifics of various consent decrees in Memphis, Chicago, and New York, which had far-reaching influence); Jerrold L. Steigman, *Reversing Reform: The Handschu Settlement in Post-September 11 New York City*, 11 J.L. & POL’Y 745, 765–70 (2003) (detailing litigation in September 2002 in which the *Handschu* consent decree was relaxed).

8. See Samuel J. Rascoff, *Domesticating Intelligence*, 83 S. CAL. L. REV. (forthcoming 2010) (discussing the involvement of state and local governments in domestic intelligence); see also, e.g., Richard A. Posner, Op-Ed., *What Our Intelligence Agencies Could Learn from Silicon Valley*, WALL ST. J., May 28, 2010, available at <http://online.wsj.com/article/SB10001424052748704717004575268783383613118.html> (noting that “there are at least 20 separate U.S. intelligence agencies, not counting state and local agencies” and that “New York City’s police department, for example, has a formidable intelligence unit”).

9. Examples abound. The so-called Lackawanna Six were Yemeni-Americans who trained in an al Qaeda camp in Afghanistan before returning to the United States with no clear follow-up plan. DINA TEMPLE-RASTON, *THE JIHAD NEXT DOOR* 175–78 (2007). The six were all convicted for their activities in Afghanistan, and the reported mastermind of the plot, Ahmed Hijazi, was killed in a Predator drone strike in Yemen. James Risen, *An American Was Among 6 Killed by U.S., Yemenis*

Say, N.Y. TIMES, Nov. 8, 2002, at A13. The "Fort Dix Six," a group of Muslim immigrants radicalized while in the United States, were convicted of conspiring to attack U.S. military personnel. See Kareem Fahim & Andrea Elliott, *In Large Immigrant Family, Religion Guided 3 Held in Fort Dix Plot*, N.Y. TIMES, May 10, 2007, at A1 (detailing the lives and families of the six immigrants). In October 2008, a Somali-American who traveled from Minneapolis to Somalia with other Somali-American youths became the first confirmed U.S. citizen to commit a suicide bombing. Andrea Elliott, *Charges Detail Road to Terror for 20 in U.S.*, N.Y. TIMES, Nov. 24, 2009, at A1. Another Somali suicide bomber may have had ties to Seattle. See Jeffrey Gettleman, *American Helped Bomb Somalia Base, Web Site Says*, N.Y. TIMES, Sept. 25, 2009, at A13 ("The Somali Web site listed a Seattle phone number for the bomber's father, but the number [was] apparently not in service."). Omar Hammami was raised a Southern Baptist in Alabama, converting to Islam and becoming increasingly radical in his viewpoints during high school. Andrea Elliott, *The Jihadist Next Door*, N.Y. TIMES, Jan. 31, 2010, (Magazine), at 26. Still in his twenties, he is currently believed to be among the leaders of Al Shabab, a Somali-militant organization linked to al Qaeda. *Id.* Concerns have grown over U.S. citizens immigrating to Yemen and associating with al Qaeda in the Arabian Peninsula. STAFF OF S. COMM. ON FOREIGN RELATIONS, 111TH CONG., AL QAEDA IN YEMEN AND SOMALIA: A TICKING TIME BOMB 1 (Comm. Print 2010). Law enforcement and intelligence officials believe that as many thirty-six American ex-convicts traveled to Yemen in 2009. *Id.* Sharif Mobley, an American man formerly employed at nuclear power plants in New Jersey, was recently arrested in Yemen on suspicion of being associated with al Qaeda in the Arabian Peninsula and also with the Somali movement Al Shabab. Scott Shane, *American's Arrest Stirs Fears That Wars Radicalize U.S. Muslims*, N.Y. TIMES, Mar. 13, 2010, at A4. Following his arrest, Mobley grabbed a security official's gun and shot two guards, one fatally. *Id.* Abdulhakim Mujahid Muhammad, born Carlos Bledsoe in Memphis, Tennessee, killed one soldier and wounded another in a shooting attack outside an army recruiting center in Little Rock, Arkansas. James Dao, *A Muslim Son, a Murder Trial and Many Questions*, N.Y. TIMES, Feb. 17, 2010, at A11. Muhammad had converted to Islam in college, becoming increasingly radicalized through studies at the Islamic Center of Nashville and a stint teaching and studying in Aden, Yemen. *Id.* Najibullah Zazi, an Afghan-born permanent resident of the United States, was arrested in September 2009 and recently pleaded guilty to attempting to detonate bombs within the New York City subway system as part of an al Qaeda plot. A.G. Sulzberger & William K. Rashbaum, *Guilty Plea Made in Plot to Bomb New York Subway*, N.Y. TIMES, Feb. 23, 2010, at A1. David Headley, a U.S. citizen "raised in elite circles in Pakistan," has been accused of assisting in the 2008 Mumbai attack by the terrorist group Lashkar-e-Taiba as well as of conspiring to attack the Danish newspaper that published cartoons of the Prophet Mohammed. Ginger Thompson & David Johnston, *U.S. Man Accused of Helping Plot Mumbai Attack*, N.Y. TIMES, Dec. 8, 2009, at A1. Headley's radicalization appears to be longstanding, and he is alleged to have received training by Lashkar-e-Taiba from 2002 to 2003. *Id.* Although the details are as yet unclear regarding the motive of the crime and its possible connection to radicalism and terrorism, Major Nidal Malik Hasan's mass murder at Fort Hood may be the most serious modern incident of homegrown radicalism and terrorism committed in the United States. See Daniel Byman, *Homeland Insecurity*, WALL ST. J., Dec. 15, 2009, available at <http://online.wsj.com/article/SB10001424052748704517504574589841594836308.html> (describing the Fort Hood shootings as "the deadliest terrorist attack on U.S. soil since 9/11"). One of the unresolved issues in the case is Hasan's relationship with Anwar al Awlaki, a Yemeni-American with alleged terrorist connections, and what influence, if any, the latter had on Hasan's subsequent crime. See *The Fort Hood Attack: A Preliminary Assessment: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs*, 111th Cong. (2009) (statement of Juan Carlos Zarate, Senior Advisor, Center for Strategic and International Studies), available at http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=70b4e9b6-d2af-4290-b9fd-7a466a0a86b6 (describing alleged communications between Hasan and al Awlaki as "troubling"); Dan Murphy, *Fort Hood Shooting: Was Nidal Malik Hasan Inspired by Militant Cleric?*, CHRISTIAN SCI. MONITOR, Nov. 10, 2009, <http://www.csmonitor.com/World/Global-News/2009/1110/fort-hood-shooting-was-nidal-malik-hasan-inspired-by-militant-cleric> (reporting that investigators are researching Hasan's contact with al Awlaki). On May 4, 2010, Faisal Shahzad, a Pakistani-born naturalized U.S. citizen, admitted involvement in a failed attempt to

carry out attacks (or attempt to) within their native or adopted country or society.¹⁰ With the rise of homegrown terrorism has also come increased discussion of radicalization—the process by which individuals or groups are socialized into a thought world that condones, valorizes, and ultimately may require acts of violence—the production cycle, so to speak, of extremist violence.¹¹ Official efforts to understand and combat this trend, which collectively go by the name “counterradicalization,”¹² have become increasingly central to American counterterrorism policy overseas as well as

detonate a car bomb in New York City’s Times Square. Mark Mazzetti et al., *Terrorism Suspect, Charged, Admits to Role in Bomb Plot*, N.Y. TIMES, May 5, 2010, at A1. In December 2009, Pakistani police arrested five U.S. citizens in the home of a man linked to radical Islamist groups. Jerry Markon et al., *Arrests Suggest U.S. Muslims, Like Those in Europe, Can Be Radicalized Abroad*, WASH. POST, Dec. 12, 2009, at A1. What the men had hoped to accomplish on their trip to Pakistan has yet to be reported. See generally RICK “OZZIE” NELSON & BEN BODURIAN, CTR. FOR STRATEGIC & INT’L STUDIES, *A GROWING TERRORIST THREAT? ASSESSING “HOMEGROWN” EXTREMISM IN THE UNITED STATES* (2010), available at http://csis.org/files/publication/100304_Nelson_GrowingTerroristThreat_Web.pdf (recounting recent incidents of domestic terrorism and suggesting measures the United States should take to counter such threats); Byman, *supra* (postulating various explanations for the recent spike in homegrown terrorists); Sebastian Rotella, *A U.S. Strain of Extremism May Be Rising*, L.A. TIMES, Dec. 7, 2009, at A1 (describing 2009 as the most dangerous year in terms of domestic terrorism since 2001); Bruce Hoffman, *American Jihad*, NAT’L INT. ONLINE, Apr. 20, 2010, <http://www.nationalinterest.org/Article.aspx?id=23200> (calling for greater official attention to the phenomenon of homegrown terrorism).

10. See CTR. ON LAW & SEC., N.Y.U. SCH. OF LAW, *TERRORIST TRIAL REPORT CARD* (2010) (demonstrating that the majority of terrorism suspects tried in federal court in the United States in the last eight years have been homegrown terrorists). There is no agreed-upon definition of homegrown terrorism. A recent report defined it as “terrorist violence perpetrated by U.S. legal residents or citizens.” NELSON & BODURIAN, *supra* note 9, at v n.1. A proposed statute, meanwhile, would have defined homegrown terrorism as “the use, planned use, or threatened use, of force or violence by a group or individual born, raised, or based and operating primarily within the United States . . . in furtherance of political or social objectives.” Violent Radicalization and Homegrown Terrorism Prevention Act of 2007, H.R. 1955, 110th Cong. § 3 (as passed by House, Oct. 23, 2007).

11. See, e.g., QUINTAN WIKTOROWICZ, *RADICAL ISLAM RISING* 5–6 (2005) (explaining how individuals in the Western world are drawn to radical Islamic groups by analyzing their initial interest in the groups, the means by which they are persuaded to believe the radical group is a credible source of Islamic interpretation, and the process by which they are persuaded to engage in “risky activism”). The homegrown terrorism that I focus on mainly emanates from certain strains of radical Islam. But the concept is certainly not limited to instances of acts of violence inspired by any one religious tradition or ideology. See, e.g., Michael Brick, *For Texas Pilot, Rage Simmered with Few Hints*, N.Y. TIMES, Feb. 19, 2010, at A1 (revealing how Joseph Stack was radicalized by antigovernment rhetoric and philosophy before flying his plane into an Austin, Texas building housing the local Internal Revenue Service offices). Joseph Stack’s suicide note clearly indicates that he wanted to be a martyr and that “violence not only [was] the answer, it [was] the only answer.” Letter from Joe Stack (Feb. 18, 2010), available at <http://graphics8.nytimes.com/packages/pdf/us/20100218-stack-suicide-letter.pdf>.

12. See, e.g., PRESIDENTIAL TASK FORCE ON CONFRONTING THE IDEOLOGY OF RADICAL EXTREMISM, *REWRITING THE NARRATIVE: AN INTEGRATED STRATEGY FOR COUNTERRADICALIZATION* 8–20 (2009) [hereinafter *REWRITING THE NARRATIVE*], available at <http://washingtoninstitute.org/pubPDFs/PTF2-Counterradicalization.pdf> (surveying efforts by European governments to address extremist ideology and offering recommendations for the U.S. government).

inside the United States.¹³ Indeed, counterradicalization is rapidly becoming a key tool for addressing homegrown terrorism before it manifests itself as violent activity.¹⁴

How should federal and local programs fit into an overarching domestic-intelligence framework in view of heightened concern about homegrown terrorism and the growing official appetite to address it through counterradicalization (and specifically through the broad-gauged intelligence that counterradicalization presupposes)?¹⁵ My claim is that given the nature

13. *See id.* at 13–17 (making numerous recommendations to the Obama Administration regarding potential changes to the United States’ counterradicalization policies in the Middle East); WHITE HOUSE, NATIONAL SECURITY STRATEGY 19 (2010) [hereinafter NATIONAL SECURITY STRATEGY], available at http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (emphasizing the need for counterradicalization efforts within the United States).

14. *See id.* at 17–18 (discussing ways to improve domestic counterradicalization efforts). In an example of the increased focus on counterradicalization, Department of Homeland Security Secretary Janet Napolitano submitted written testimony to the Senate Homeland Security Committee detailing the efforts by the Department, especially its Office of Information and Analysis (I&A), to counter radicalization, noting that I&A “strengthen[ed] its analysis in several areas,” notably “violent radicalization and domestic terrorism.” *Eight Years After 9/11: Confronting the Terrorist Threat to the Homeland: Hearing Before the S. Comm. on Homeland Security & Governmental Affairs*, 111th Cong. (2009) (statement of Janet Napolitano, Secretary, Department of Homeland Security), available at http://www.dhs.gov/ynews/testimony/testimony_1254321524430.shtm. More generally, in his Nobel Prize acceptance speech, President Obama referred to radicalization as a major threat to peace which must be countered by a correct understanding of faith as “the law of love”:

[G]iven the dizzying pace of globalization, the cultural leveling of modernity, it perhaps comes as no surprise that people fear the loss of what they cherish in their particular identities—their race, their tribe, and perhaps most powerfully their religion. In some places, this fear has led to conflict. . . . [M]ost dangerously, we see it in the way that religion is used to justify the murder of innocents by those who have distorted and defiled the great religion of Islam, and who attacked my country from Afghanistan.

Barack Obama, U.S. President, Remarks by the President at the Acceptance of the Nobel Peace Prize (Dec. 10, 2009), <http://www.whitehouse.gov/the-press-office/remarks-president-acceptance-nobel-peace-prize>. Counterradicalization, which is strategic in its breadth and anticipatory in its methodology, can be distinguished from deradicalization, which aims to unwind ideological developments that have already taken place within an individual or group. OMAR ASHOUR, THE DE-RADICALIZATION OF JIHADISTS 5–6 (2009). In an interview with *Der Spiegel*, Napolitano said that the United States will expand its communication and coordination with Europe regarding deradicalization, as both face similar questions: “How do you identify a youth who is susceptible to becoming radicalized? How do you work with that youth, his family and community to give them alternatives to radicalization?” Cordula Meyer, *Away from the Politics of Fear*, DER SPIEGEL ONLINE, Mar. 16, 2009, <http://www.spiegel.de/international/world/0,1518,613330,00.html>.

15. *See supra* notes 12–14 and accompanying text. There are reasons to be concerned about the abilities of both federal and local programs. Counterradicalization implies the capacity of officials to comprehend and intervene in processes that are heavily informed by religiously inspired ideology, historically not a strong suit of law enforcement agencies. *See* RICHARD A. POSNER, COUNTERING TERRORISM 105–10 (2007) (discussing how law enforcement and intelligence agencies diverge in terms of their missions and institutional cultures). A debate rages across Western European democracies (many of which currently practice counterradicalization more vigorously and comprehensively than the United States) about the degree to which nonviolent extremists ought to be enlisted in the ideological struggle against violent extremists. *See, e.g.,*

of contemporary counterterrorism intelligence, exclusive—or even excessive—reliance on federal modalities is mistaken.¹⁶ I argue that a properly conceived approach to homegrown terrorism should leverage three main comparative strengths possessed by local intelligence. First, local intelligence has proved especially adept at supplying a conceptual framework for thinking about, and addressing, homegrown terrorism. I refer to the ability of local officials to “see” the threat in terms of local phenomena as an example of “epistemic federalism.” Second, local officials excel at what I call (following Elinor Ostrom) “coproduction” of intelligence, a form of collaborative intelligence gathering and interpretation that enlists the support of local populations.¹⁷ Third, owing to informal mechanisms and incentives, local police may be more likely to carry out aspects of their intelligence missions with greater attentiveness to issues of basic rights.

But local intelligence has its limitations and comparative disadvantages as well. First, I contend that local intelligence officials lack the analytic capacity to make full use of their institutional strengths as intelligence collectors.¹⁸ Second, for all that certain informal incentives may tend to

Lorenzo Vidino, *Europe's New Security Dilemma*, WASH. Q., Oct. 2009, at 62 (“A source of particularly heated debate among policymakers is the role that could be played in these programs by nonviolent Islamists . . .”). Furthermore, as discussed below, counterradicalization implicates concerns about basic freedoms guaranteed by the Bill of Rights, especially those embodied in the First Amendment’s Speech and Religion Clauses. See *infra* notes 112–13 and accompanying text. For a recent powerful critique of British counterradicalization policy, see ARUN KUNDNANI, SPOOKED! HOW NOT TO PREVENT VIOLENT EXTREMISM (2009), <http://www.irt.org.uk/pdf2/spooked.pdf> and COMMUNITIES AND LOCAL GOV’T COMM., PREVENTING VIOLENT EXTREMISM, 2009–2010, H.C. 65, 8–23 (criticizing official U.K. counterradicalization policy for various counterproductive and legally questionable practices).

16. I do not mean to argue that federal intelligence does not possess formidable advantages over local intelligence. Federal officials are vastly more experienced and capable in areas of electronic surveillance, including tracking material on the Internet. See DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 3 (2007) (summarizing the history of federal national-security surveillance from the expiration of a World War I statute barring federal wiretapping in 1919 to the War on Terror). Furthermore, although the NYPD has dispatched approximately ten of its intelligence officers to overseas posts, Adam Pincus, *Traveling Blues: Oversight Procedures on Expenses and Legal Issues Unclear for Overseas NYPD Officers*, CITY HALL, Mar. 10, 2008, <http://www.cityhallnews.com/newyork/article-285-traveling-blues.html>, it obviously remains the case that the federal government enjoys a massive intelligence advantage beyond the nation’s borders. See KRIS & WILSON, *supra*, at § 16:2 (describing federal authority to conduct intelligence activities abroad).

17. See Elinor Ostrom, *Organizational Economics: Applications to Metropolitan Governance*, 6 J. INSTITUTIONAL ECON. 109, 111 (2010) (arguing that coproduced services are provided most effectively by smaller departments that make relationships with their citizens and learn the differences between neighborhoods). Like the much more widely discussed idea of counterinsurgency, counterradicalization places emphasis on interactions between government and more general populations. Cf. MICHAEL T. FLYNN ET AL., CTR. FOR A NEW AM. SEC., FIXING INTEL: A BLUEPRINT FOR MAKING INTELLIGENCE RELEVANT IN AFGHANISTAN 4 (2010) (arguing against excessive reliance on intelligence related to insurgent violence and in favor of more broad-gauged intelligence related to “fundamental questions about the environment in which [U.S. forces] operate and the people [U.S. forces] are trying to protect and persuade”).

18. The intelligence cycle is an iterative process that includes, most basically, collection and analysis. See MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 51 (2d ed. 2003)

impose salutary restraints on aspects of local intelligence, formal governance mechanisms to ensure that the intelligence work they carry out is respectful of basic rights (and accurate) are largely absent. I thus argue for the creation of new federal–local collaborative structures that will simultaneously enhance the analytic rigor and the legal oversight of local intelligence while leaving undisturbed and exploiting to full effect the advantages that local intelligence possesses.

Others have made ambitious, even extravagant, claims on behalf of local police and their role in intelligence.¹⁹ Indeed, such claims have, in some sense, become a staple of contemporary American counterterrorism discourse.²⁰ But regardless of whether these claims have been advanced by policy makers, commentators, or officials, they have typically ignored the issue of precisely what the local police do or should be doing under the banner of intelligence. Instead, claims of local excellence have frequently been limited to clichés about the sheer number of subfederal police departments and officers across the country and their ability to serve as “eyes and ears” of the nation.²¹ These accounts often emphasize, without analysis (and indeed,

(describing the intelligence cycle as a “perfect circle” in which the intelligence community “collects intelligence, which is then processed and exploited, analyzed and produced, and disseminated to the policymakers”).

19. See, e.g., CHRISTOPHER DICKEY, *SECURING THE CITY: INSIDE AMERICA’S BEST COUNTERTERROR FORCE—THE NYPD* (2009) (presenting a narrative portraying the NYPD as the nation’s most effective counterterrorism force); William Finnegan, *The Terrorism Beat: How Is the N.Y.P.D. Defending the City?*, *NEW YORKER*, July 25, 2005, at 58, 61 (quoting RAND expert Brian Jenkins as saying that “[a]s [international terrorism] metastasizes, . . . [w]e’re going to win this at the local level”). My focus throughout is on the role of police (federal and local) in intelligence gathering and analysis. Obviously, intelligence does not exhaust the role of police in counterterrorism work. For a thoughtful survey of some of the conceptual issues brought up by the involvement of local police in counterterrorism, see generally Matthew C. Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, 3 *J. NAT’L SECURITY L. & POL’Y* 377 (2009).

20. See, e.g., *Radicalization, Information Sharing and Community Outreach: Protecting the Homeland from Homegrown Terror: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong. 12 (2007) (statement of William J. Bratton, Chief of Police, Los Angeles Police Department) (“[O]ver 700,000 local law enforcement officers in the U.S. are already on the front lines, fighting crime and gathering critical information on a daily basis.”).

21. Comments like those of former Director of National Intelligence John Negroponte are typical:

We all recognize that—while protecting the rights of our citizen—critical terrorism information can be developed by engaged police officers who patrol the streets of our nation. In fact, without engaged police officers, we may not stop the next threat. The federal government can’t be—and shouldn’t try to be—everywhere all the time. We rely mightily on the more than 13,000 state and local police departments in the United States. Our state and local colleagues are our eyes and ears throughout the nation.

John D. Negroponte, Dir. Nat’l Intelligence, Remarks to the FBI National Academy 2 (Oct. 3, 2006), available at www.dni.gov/speeches/20061003_speech.pdf; see also Dennis C. Blair, Op-Ed, *Strengthening Our Front Line of Defense*, *WASH. POST*, Dec. 18, 2009, at A31 (touting increased co-operation among FBI, local law enforcement, and intelligence agencies in the recent arrests of Americans allegedly associated with foreign terrorist organizations).

increasingly without basis in fact), that intelligence collection and criminal investigation are synergistic, as if to say that local police can engage in intelligence work passively as an incident of their primary anticrime responsibilities.²² And while certain other accounts have tended to be more precise in distinguishing between criminal investigation and pure intelligence, they have typically concluded that local officials lack the ability to engage in genuine intelligence work and inevitably turn (both as a matter of description and prescription) to their federal counterparts where intelligence is required. For example, a leading study on the subject of the role of local law enforcement in intelligence observes that federal authorities “will naturally lead in intelligence gathering that is not connected to criminal investigation” because local law enforcement agencies “have neither money nor capacity for that kind of pure intelligence.”²³ Both the excessively general accounts purporting to celebrate police intelligence and the more sophisticated treatments casting aspersions on the ability of the police to engage in true intelligence miss something important. In view of the emergence of homegrown terrorism and the mounting official preoccupation with counterradicalization, local police are well positioned—arguably better so than their federal counterparts—to engage in genuine intelligence work.²⁴

Another body of literature touts the ability of local officers to serve as effective guardians of liberty in the counterterrorism area, for a number of interrelated reasons. Some accounts have emphasized the capacity of local police to resist, on federalism grounds, overbearing federal counterterrorism initiatives.²⁵ Other narratives emphasize the presence of various informal or

22. As discussed below, counterradicalization intelligence substantially loosens any requirement for tying authority to engage in intelligence gathering to a finding of even potential criminal liability. See *infra* note 78 and accompanying text. For a discussion of the distinction between high (intelligence and security-related) and low (case-oriented) policing, see Jean-Paul Brodeur, *High and Low Policing in Post-9/11 Times*, 1 POLICING 25, 26 (2007).

23. K. JACK RILEY ET AL., STATE AND LOCAL INTELLIGENCE IN THE WAR ON TERRORISM, at xiv–xv (2005). While the report may be accurate (especially as to funding) as a descriptive matter, its conclusion is flawed in view of the fact that it is predicated on an excessively narrow, technology-based view of intelligence. See *id.* at 2 (distinguishing between “intelligence gathering” and “information gathering” on the basis of the use of electronic surveillance).

24. Contemporary European practice is of a piece with this claim. For example, “Rich Picture” represents a collaboration between local police and the British Security Service (MI5). See Gordon Corera, *Don't Look Now, Britain's Real Spooks Are Right Behind You*, TIMES ONLINE, Dec. 2, 2007, <http://www.timesonline.co.uk/tol/news/uk/article2982769.ece> (“The counterterrorist machinery has also spread out from London around the country, with a series of large regional MI5 stations opening to work closely with the police. . . . A joint project, Rich Picture, is designed to cast a wide intelligence net to pick up warning signs of radicalisation or unusual activity as early as possible.”).

25. See, e.g., Ernest A. Young, *Welcome to the Dark Side: Liberals Rediscover Federalism in the Wake of the War on Terror*, 69 BROOK. L. REV. 1277, 1290–91 (2004) (arguing that “[f]ederalism best protects liberty over time” by providing “potential dissenters [to federal counterterrorism strategies]. . . their own [state] governmental institutions around which to organize their efforts, as well as their own constitutional space in which to implement and demonstrate the effectiveness of alternative policies”).

indirect accountability mechanisms at the local level, ranging from robust media presences to local elections, as a check on local counterterrorism practices.²⁶ Still others focus on the presence of incentives that cause local police to be more respectful of community viewpoints and sensitivities than federal officials.²⁷ While each of these theories (especially the third) has some explanatory power, the comparative advantages, in terms of liberty protection, of intelligence practiced by local officials should not be overstated. Even more so than federal intelligence, local intelligence operates in a governance vacuum.²⁸ A generation ago, governance of local intelligence agencies was furnished to a large degree by federal courts that had jurisdiction over consent decrees that resolved civil rights actions against police intelligence agencies.²⁹ In recent years, those decrees have been sharply scaled back, if not discontinued.³⁰ My account pays close attention to the vulnerability of rights in a world in which formal governance mechanisms are not fully operative.

My argument unfolds as follows. In Part I, I set out in detail the two main theoretical bases for local success in contemporary counterterrorism intelligence: the distinctive ability of local officials to “see” the threat of homegrown terrorism through a process that I refer to as epistemic federalism,³¹ and their advantage in coproducing intelligence with members of the community in furtherance of counterradicalization. I also draw attention to the main limits of local intelligence effectiveness, namely the absence of analytic capacity, intelligence training, and budgets.

Part II explores the ways in which local intelligence may be well positioned to protect rights largely through informal mechanisms and incentive structures. At the same time, it also observes that local intelligence—even more so than federal—operates within a governance vacuum, a potentially worrisome state of affairs given documented historical abuses on the part of local police intelligence.

26. See, e.g., Jerome H. Skolnick, *Democratic Policing Confronts Terror and Protest*, 33 SYRACUSE J. INT’L L. & COM. 191, 211 (2005) (emphasizing New York’s “institutions of accountability”).

27. See, e.g., Daniel Richman, *The Right Fight: Enlisted by the Feds, Can Police Find Sleeper Cells and Protect Civil Rights, Too?*, BOSTON REV., Dec. 2004–Jan. 2005, available at <http://bostonreview.net/BR29.6/richman.php> (discussing the central role of local law enforcement in ensuring public safety as part of a balanced “portfolio” which helps local officials in dealing with community leaders).

28. See *infra* Part II.

29. See Chevigny, *supra* note 7, at 751–67 (discussing the circumstances leading up to and the specifics of various consent settlement decrees in Memphis, Chicago, and New York that had far-reaching influence).

30. See *infra* notes 116–17 and accompanying text.

31. See *infra* notes 38–44 and accompanying text.

Part III brings the analysis from the conceptual to the institutional. Owing in part to political pressure,³² the national-security bureaucracy in Washington has been mobilized to engage local and state law enforcement as part of an overall counterterrorism effort.³³ The Department of Homeland Security (DHS), the Office of the Director of National Intelligence (ODNI), the FBI, and other agencies and branches of agencies are now involved in this sort of “outreach.”³⁴ But for all of these efforts, it is hard to say with confidence what the collaboration between federal and subfederal actors in this area has achieved, or even what, specifically, it is meant to achieve. I pay attention to the role of three core collaborative programs—FBI Joint Terrorism Task Forces³⁵ (JTTFs), DHS Fusion Centers,³⁶ and the Interagency Threat Assessment and Coordination Group (ITACG) (housed within the National Counterterrorism Center (NCTC) within the ODNI)³⁷—designed in large measure to coordinate local and federal intelligence work, and I criticize each of them for various inadequacies. The JTTFs essentially co-opt local officers, functionally rendering them federal officers and depriving them of the distinctive strengths possessed by members of local departments. The Fusion Centers are predicated on a devolution of intelligence from the center to the periphery, but the wrong function—intelligence sharing, rather than collection and analysis—is devolved. The ITACG, by embedding local officials within the nerve center of U.S. counterterrorism intelligence, comes closer in concept to achieving a workable and useful model, but the program places too much emphasis on local consumption of federal intelligence. I go on to adumbrate what a more successful set of collaborative institutions would look like, emphasizing the need for federal–local co-operation that enhances analytic rigor and ensures fidelity to law at the local level.

32. For an example of an association advocating more involvement of local law enforcement in homeland security and intelligence, see MAJOR CITIES CHIEFS ASS’N, TWELVE TENETS TO PREVENT CRIME AND TERRORISM 6 (2008), available at <http://www.majorcitieschiefs.org/pdfpublic/MCC%20Twelve%20Tenet%20Final%205%2021%2008.pdf>.

33. See *infra* subpart III(A).

34. See *infra* subpart III(A). For example, within DHS, the Office of Intelligence and Analysis is responsible for both the Fusion Centers formally tasked with sharing information with state and local jurisdictions and the broader policy of information sharing with subnational units. *FY2010 Budget Request: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 111th Cong. (2009) (statement of Bart R. Johnson, Acting Under Secretary, Office of Intelligence and Analysis, Department of Homeland Security).

35. Federal Bureau of Investigation, Protecting America Against Terrorist Attack: A Closer Look at Our Joint Terrorism Task Forces, http://www.fbi.gov/page2/may09/jtfts_052809.html.

36. Department of Homeland Security, State and Local Fusion Centers, http://www.dhs.gov/files/programs/gc_1156877184684.shtm (last modified Sept. 16, 2009).

37. Interagency Threat Assessment and Coordination Group, <http://www.ise.gov/docs/misc/ITACG-brochure.pdf>.

I. Local Intelligence and Effectiveness

A. *Epistemic Federalism and Homegrown Terrorism*

Local counterterrorism intelligence may seem like a contradiction in terms. After all, terrorism is ostensibly a global phenomenon underwritten by a global ideology.³⁸ Local efforts would seem to be in tension with what scholars in another area have referred to as the “matching principle,” according to which “the size of the geographic area affected by a specific [problem] should determine the appropriate governmental level for responding to the [problem].”³⁹ As one commentator has put it, “no city interest counterbalances the burdens of police surveillance.”⁴⁰ One sense in which

38. See Lawrence C. Reardon, *Interpreting Political Islam's Challenge to Southeast Asia*, in *DEMOCRATIC DEVELOPMENT AND POLITICAL TERRORISM* 195, 213 (William Crotty ed., 2005) (“Radical Islamic terrorism thus is viewed as a transnational phenomenon that had been transformed from a local to a regional or global phenomenon.”). As mentioned, I am focusing primarily on homegrown terrorism related to certain varieties of radical Islam, although the concepts discussed in the Article could be applied equally to combating homegrown terrorism inspired by any ideology.

39. Henry N. Butler & Jonathan R. Macey, *Externalities and the Matching Principle: The Case for Reallocation Environmental Regulatory Authority*, 14 *YALE L. & POL'Y REV.* 23, 25 (1996). For a city to practice counterterrorism, just as for a state like California to regulate greenhouse gases with an eye to redressing global warming, is to devote resources to a problem that by its nature eludes comprehensive local resolution. For a view that terrorism “must be added to the Constitution’s list of piracy and treason as unassailable redoubts of federal concern,” see Elizabeth Glazer, *A New World*, *BOSTON REV.*, Dec. 2004–Jan. 2005, available at <http://bostonreview.net/BR29.6/glazer.php>.

40. David Thacher, *The Local Role in Homeland Security*, 39 *LAW & SOC'Y REV.* 635, 669 (2005) (emphasis omitted). In the specific case of the NYPD, certain aspects of its counterterrorism program may have been designed, in part, to motivate the federal government to take similarly aggressive action, a sort of reversal of the famous Brandeisian laboratory theory of federalism in the sense that here the subnational entity played the role not of laboratory rat but of provocateur. See DICKEY, *supra* note 19, at 157–59 (giving examples of the NYPD’s more aggressive intelligence-gathering techniques that the FBI later adopted). The directive issued by FDR referenced in the introductory paragraph, itself the result of a memo written by FBI Director Hoover to Attorney General Frank Murphy on March 6, 1939, reveals a similar tension. See CT READER, *supra* note 1, at 171–72 (reporting that the sequence of events that led to FDR’s issuance of the directive began with Hoover’s memo). In that memo Hoover explained that the federal government needed to become more active in countersabotage operations because the public was beginning to assume that it was the local—and not the federal—government which would be in the lead. *Id.* Hoover had learned that the NYPD had “created a special sabotage squad of fifty detectives . . . and that this squad [would] be augmented in the rather near future to comprise 150 men.” *Id.* at 171. There had been “considerable publicity” with the result that private citizens were likely to transmit information concerning sabotage “to the New York City Police Department rather than the FBI.” *Id.* After informing the Attorney General of this development, “the Director strongly urged that the President ‘issue a statement or request addressed to all police officials in the United States: asking them to turn over to the FBI ‘any information obtained pertaining to espionage, counterespionage, sabotage, and neutrality regulations.’” *Id.* Similarly, as Richard Stewart has underscored, there are rational explanations for violations of the “matching principle” on the part of subnational actors addressing climate change. Richard B. Stewart, *States and Cities as Actors in Global Climate Regulation: Unitary vs. Plural Architectures*, 50 *ARIZ. L. REV.* 681, 691 (2008). First, subnational governments that lead in this area will achieve “radiator effects” by stimulating participation by other states, thereby spreading costs and increasing benefits. *Id.* Second, subnational agencies that assume

the matching problem has been ameliorated, if not entirely overcome, by local efforts at counterterrorism intelligence is connected to what I refer to as epistemic federalism.⁴¹ Institutions inevitably approach issues from distinctive perspectives as a function of their own capacities.⁴² Local agencies “see” the local factors of terrorism more clearly than national agencies that view the world through the prism of global trends.⁴³ Epistemic federalism has proved especially valuable in conceptualizing the threat from contemporary terrorism as a function of certain path-dependent truths about the nature of the threat and the nature of local intelligence capabilities.⁴⁴

leadership roles may be able to leverage their market position by causing other subnational groups to piggyback on their policies. *Id.* at 692. Third, there may be a race to the top in which benefits accrue to industry in greenhouse-gas-regulation-leader jurisdictions. *Id.* at 691. *But see* Jonathan B. Wiener, *Think Globally, Act Globally: The Limits of Local Climate Policies*, 155 U. PA. L. REV. 1961, 1965 (2007) (arguing that a race to the bottom is more likely than a race to the top); Dafna Linzer, *In New York, a Turf War in the Battle Against Terrorism*, WASH. POST, Mar. 24, 2008, at A1 (discussing the conflicts between the NYPD and the FBI). Many of the clashes Linzer describes date back two or three years and have been adequately addressed by the FBI more recently. *See id.* (“[R]ecently, officials in the FBI and the NYPD said the bitterness . . . [had] faded. . . . Both departments credit the improvement to a pivotal meeting, 2 1/2 years ago, between [Police Commissioner] Kelly and FBI Director Robert S. Mueller III.”).

41. Epistemic federalism diverges from the view that questions of institutional design are logically anterior to questions of understanding the threat. For an opposite view that politics play a greater role in the process, see William Stuntz, *Responses to the September 11 Attacks: Terrorism, Federalism, and Police Misconduct*, 25 HARV. J.L. & PUB. POL’Y 665, 670–71 (2002).

42. *See* William N. Eskridge, Jr. & John Ferejohn, *Structuring Lawmaking to Reduce Cognitive Bias: A Critical View*, 87 CORNELL L. REV. 616, 620–21 (2002) (discussing psychological literature as it relates to decisional biases).

43. As NYPD Deputy Commissioner Richard Falkenrath has observed in Congressional testimony,

In combating ‘homegrown’ threats, the burden shifts . . . almost entirely to local law enforcement. . . . This is one of the reasons why the NYPD has decided to augment its joint counterterrorism investigative work with the FBI with an organizationally distinct intelligence program operating under separate legal authorities.

Homeland Security: The Next Five Years: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs, 109th Cong. 19 (2006) (statement of Richard Falkenrath, Deputy Comm’r, New York City Police Department) [hereinafter Falkenrath, *Hearing*], available at http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=9f137c90-5424-4bc6-a3eb-f785acc1f82d.

44. Epistemic federalism argues for an interdisciplinary approach to problem solving that leverages the various informational capacities of government at different levels to achieve a more complete overall understanding of a phenomenon. The concept of epistemic federalism resonates with Schapiro’s concept of “polyphonic federalism” that leverages the competitive overlap between national and subnational governments. *See* Robert A. Schapiro, *Toward a Theory of Interactive Federalism*, 91 IOWA L. REV. 243, 244 (2005) (“Polyphonic federalism does not divide state and federal authority, but instead seeks to harness the interaction of state and national power to advance the goals associated with federalism.”). The core Executive Order that guides the work of the Intelligence Community also builds in this competitive impulse. *See* Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008) (recognizing the value of analytic competition between intelligence agencies for generating sound intelligence), *reprinted as amended in* 50 U.S.C. § 401 (2006). But epistemic federalism is subtly yet fundamentally different in that it views the subnational actors not

Epistemic federalism draws its explanatory force from the fact that it is more faithful to the reality and the self-conception of the emergent trend of homegrown terrorism. While Washington (especially in the years immediately following 9/11) has tended to project a high level of formality and organizational structure onto al Qaeda,⁴⁵ much of what we refer to as al Qaeda has actually been transformed into a loosely knit network linking informal “groups of guys” who are becoming radicalized in neighborhood organizations and are recruiting themselves to participate in acts of terrorist violence.⁴⁶ Indeed, such a network structure may reflect a deliberate strategic choice.⁴⁷ Thus, the foremost ideologue of the contemporary jihad explicitly rejects the idea of the centralized, secret organization, advocating instead for a loosely networked system of action.⁴⁸

The groups of guys (or clusters) begin, as Bernard Rougier has noted, with “idle teenagers who [have] been resocialized by radical religious networks.”⁴⁹ Unchecked, the cluster may be transformed into an operational team that is capable of taking violent action.⁵⁰ And as Marc Sageman has written, it may be the building block of a global-networked enemy: “The process of radicalization that generates small, local, self-organized groups in a hostile habitat but linked through the Internet also leads to a disconnected global network . . . [which is] the natural outcome of a bottom-up mechanism of group formation”⁵¹

merely as alternative regulatory actors to the federal government but as institutional actors possessed of different perspectives on regulatory problems.

45. See, e.g., James Risen & David Johnston, *Al Qaeda May Be Rebuilding in Pakistan, E-mails Indicate*, N.Y. TIMES, Mar. 6, 2002, at A1 (“American officials believe that one of the benefits of the war in Afghanistan was to disrupt the terror network’s ability to communicate from a central command center.”).

46. See MARC SAGEMAN, *LEADERLESS JIHAD* 141 (2008) (describing the lack of formality in local networks). Sageman’s thesis has been criticized, especially by Bruce Hoffman, who regards al Qaeda as posing an enduring threat as a headquarters organization. See Bruce Hoffman, *The Myth of Grass-Roots Terrorism*, 87 FOREIGN AFF., May–June 2008, at 133, 134–35 (citing governmental authorities who contend that al Qaeda remains America’s most serious threat and retains top-down command capabilities).

47. See SAGEMAN, *supra* note 46, at 143 (“The process of radicalization that generates small, local, self-organized groups in a hostile habitat but linked through the Internet also leads to a disconnected global network, the leaderless jihad.”).

48. See BRYNJAR LIA, *ARCHITECT OF GLOBAL JIHAD: THE LIFE OF AL-QAIDA STRATEGIST ABU MUS’AB AL-SURI* 104 (2008) (excerpting a 1991 audiotape by Abu Mus’ab al-Suri, in which al-Suri discusses the need for global jihad to eliminate vulnerable command structures, prefiguring the organizational slogan he later developed, “*nizam la tanzim*,” meaning “system, not organization”).

49. BERNARD ROUGIER, *EVERYDAY JIHAD* 276 (2007).

50. See *id.* at 277 (“If . . . nothing is done to resume Palestinian-Israeli negotiations, Ain al-Helweh might become the vanguard of a salafist-jihadist militancy that would spread in the Palestinian territories, break through nationalist barriers, and change the scale of the struggle, the better to strike ‘the serpent’s head’”).

51. SAGEMAN, *supra* note 46, at 143. “The global Salafi jihad has a very fuzzy boundary . . . [which] raises . . . epistemological issues on a group and individual level.” MARC

If the cluster supplies the sociological building blocks of the threat, then the “node” supplies its micro-geography; it is at the node where the radicalization first takes place.⁵² In Rougier’s Ain al-Hilweh refugee camp, it is a mosque, a bookstore, a media outlet.⁵³ In the Jemaa al-Mezuak neighborhood of Tetouan, Morocco, it is the mosque, whose Imam has dispatched a dozen young men into Iraq to serve as suicide bombers.⁵⁴ In Leeds, where the July 7, 2005 London suicide bombers became radicalized, it was a local bookshop and a fitness facility dubbed the “Al Qaeda gym.”⁵⁵

If the contemporary jihad is increasingly organized around small groups of men who become radicalized at certain virtual and bricks-and-mortar nodes, it stands to reason that local police are well positioned to gather intelligence about the threat. As Marc Sageman has explained, an effective intelligence methodology

should focus precisely on how the terrorists act on the ground: how they evolve into terrorists; how they interact with others (terrorists and nonterrorists); how they join terrorist groups; how they become motivated to commit their atrocities; how they are influenced by ideas; and how they follow orders from far-away leaders. These questions call for a perspective from the bottom up to see exactly what is happening on the ground in the hope of explaining the larger phenomenon of terrorism.⁵⁶

Local police departments typically enjoy three important structural advantages in pursuing this “bottom up” perspective.⁵⁷ First, they have

SAGEMAN, UNDERSTANDING TERROR NETWORKS 151 (2004). The homegrown threat is not limited to the United States or to its Western European allies. Bernard Rougier, whose study of Islamic radicalization in the Lebanese refugee camp Ain al-Hilweh offers a powerful case study of the local origins of jihad, has written, “Whatever the nature of the ties between Islamists in Lebanon—or some of them—and Osama bin Laden or Ayman al-Zawahiri, the salafist-jihadist phenomenon exists autonomously: its development does not depend on ‘international terrorist networks.’” ROUGIER, *supra* note 49, at 275.

52. The node may be a physical location or a virtual one. See STAFF OF S. COMM. ON HOMELAND SEC. AND GOVERNMENTAL AFFAIRS, 110TH CONG., VIOLENT ISLAMIST EXTREMISM, THE INTERNET, AND THE HOMEGROWN TERRORIST THREAT 15 (2008) [hereinafter VIOLENT ISLAMIST EXTREMISM], available at http://hsgac.senate.gov/public/_files/IslamistReport.pdf (“Despite recognition in the [National Implementation Plan] that a comprehensive response is needed, the U.S. government has not developed nor implemented a coordinated outreach and communications strategy to address the homegrown terrorist threat, especially as that threat is amplified by the use of the Internet.”).

53. See ROUGIER, *supra* note 49, at 86–98 (describing the methods by which the al-Nur and Salah al-Din Mosques, al-Huda bookstore, and *al-Hidaya* newspaper provided access to radicalization theories and materials to refugees).

54. Andrea Elliott, *Where Boys Grow Up to Be Jihadis*, N.Y. TIMES, Nov. 25, 2007, (Magazine), at 70; Fiona Govan, *Town That Breeds Suicide Bombers*, DAILY TELEGRAPH, Nov. 25, 2006, at 16.

55. Christopher Caldwell, *After Londonistan*, N.Y. TIMES, June 25, 2006, § 6 (Magazine), at 41.

56. See SAGEMAN, *supra* note 46, at 23–24.

57. Cf. Richard H. Shultz Jr. & Roy Godson, *Intelligence Dominance: A Better Way Forward in Iraq*, WKLY. STANDARD, July 31, 2006, at 22, 24 (referring to a veteran foreign intelligence professional who “was describing a situation in which an operative functions somewhat like the

comparatively large staffs. The example of the NYPD is suggestive.⁵⁸ As against the FBI's approximately 13,500 Special Agents nationwide,⁵⁹ who typically spend between three and five years in any given office before being rotated to another,⁶⁰ the NYPD deploys 34,500 officers in the five boroughs of New York City alone.⁶¹ Second, local police possess the cultural and linguistic diversity that affords them access to the communities most susceptible to penetration by radical ideology.⁶² While federal intelligence agencies struggle to find individuals who speak Arabic, Persian, or Urdu, the NYPD has no shortage of individuals who speak these languages and can reach out to, or immerse themselves in, ethnic and religious communities.⁶³

policeman on the beat—constantly talking to, interacting with, and keeping tabs on the people in his neighborhood and, most of all, keeping his eyes open for slight changes or new developments in the local scene”).

58. It goes without saying that the NYPD does not supply a model of local intelligence that can be replicated in every respect by other major metropolitan, still less (the more typical) suburban or rural police departments. Still, it is useful to discuss the NYPD as offering a conceptual alternative to federal intelligence, both in terms of its institutional strengths and vulnerabilities.

59. Federal Bureau of Investigation, About Us—Quick Facts, <http://www.fbi.gov/quickfacts.htm>.

60. Daniel Richman, *Prosecutors and Their Agents, Agents and Their Prosecutors*, 103 COLUM. L. REV. 749, 788–89 (2003).

61. NYPD Frequently Asked Questions, http://www.nyc.gov/html/nypd/html/faq/faq_police.shtml.

62. See Colleen Long, *US Police Departments Seeking More Bilingual Cops*, DAILYNEWS, Mar. 11, 2010, http://news.yahoo.com/s/ap/20100311/ap_on_re_us/us_bilingual_cops_2 (noting that one-third of NYPD employees can speak a second language—of those, “785 are certified linguists or expert translators in 63 languages, including Bengali, Dari, Farsi, Arabic and Urdu”). As of March 2010, the Minneapolis Police Department has a dedicated Crime Prevention Specialist who speaks Somali. See Minneapolis Police Department Sector Lieutenant & Crime Prevention Specialist Contacts, <http://www.ci.minneapolis.mn.us/safe/docs/safe-staff-map.pdf> (listing a Somali contact under cultural outreach).

63. See *supra* note 62. “The FBI did not dedicate sufficient resources to the surveillance and translation needs of counterterrorism agents. It lacked sufficient translators proficient in Arabic and other key languages, resulting in significant backlog of untranslated intercepts.” NAT’L COMM’N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 77 (2004) [hereinafter 9/11 COMMISSION REPORT]. Security concerns also increased the difficulty of recruiting officers qualified for counterterrorism. “Very few American colleges or universities offered programs in Middle Eastern languages or Islamic studies Anyone who was foreign-born or had numerous relatives abroad was well-advised not even to apply.” *Id.* at 92. “Similar to our findings in our previous audits, we determined that the FBI still does not have a reliable means of assessing the amount of foreign language audio, text, and electronic material it collects and reviews for its counterterrorism, counterintelligence, and criminal operations.” OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, AUDIT REPORT 10-02, THE FEDERAL BUREAU OF INVESTIGATION’S FOREIGN LANGUAGE TRANSLATION PROGRAM 48 (2009), available at http://www.justice.gov/oig/reports/FBI/a1002_redacted.pdf. As the *New York Times* has reported,

The report also contains new information about the bureau’s efforts to hire more translators. It showed that the number of the bureau’s linguists—both staff members and contractors—had fallen slightly to 1,298 as of September 2008, from a peak in 2005. It met its hiring targets in 2008 for only 2 of 14 targeted languages.

The process of hiring linguists has been slowed because of lengthy security vetting and competition with other intelligence agencies that are also trying to hire more translators, the report said.

Third, local police departments also have a broad mandate—embodied in the familiar motto “to serve and protect”—rather than circumscribed authority merely to enforce the law.⁶⁴ Like other local departments, the NYPD’s officers are mainly on patrol—generalist cops who walk a beat and develop complex understandings of, and working relationships with, the community.⁶⁵ The FBI, meanwhile, has historically vacillated between conceiving of itself as a detective bureau with authority to investigate the violation of specific federal criminal statutes, and regarding itself (as it currently does) as also having the mandate to gather intelligence even absent criminal predication.⁶⁶

In sum, the epistemic advantage of local police in conceptualizing and tracking the threat of homegrown terrorism draws on the distinctive capacities and authorities that local police departments possess. Local counterterrorism intelligence has been uniquely well positioned to see the emergence of the threat on the microlevel.⁶⁷ Whether by focusing on and

Charlie Savage, *F.B.I. Is Slow to Translate Intelligence, Report Says*, N.Y. TIMES, Oct. 27, 2009, at A20. The lack of native language speakers in the FBI is largely an artifact of the national-security clearance process, a holdover from the Cold War where the presence of relatives in a sensitive location overseas would tend to disqualify an individual from obtaining a clearance. See OFFICE OF THE INSPECTOR GEN., *supra*, at 77 (noting that the length of the clearance process for linguists, averaging fourteen months, is even longer for foreign-born linguists with family still living abroad). While critics rail against the anachronistic clearance process, it remains a fact of life in the federal Intelligence Community and is unlikely to change soon. Cf. DIR. OF NAT’L INTELLIGENCE, U.S. INTELLIGENCE CMTY., FOLLOW-UP REPORT ON 100 DAY PLAN: INTEGRATION AND COLLABORATION 14–15 (2007) (suggesting means to address the “[m]ultiple, complex, and inconsistent security clearance systems” that “slow the pace in filling open positions and moving personnel”). Willy-nilly, this has given local intelligence a comparative institutional advantage—so much so that the “[t]he Department of Defense recently borrowed seventeen computer-literate Arabic speakers from the N.Y.P.D. to assist its intelligence arm.” Finnegan, *supra* note 19, at 64.

64. See Steven M. Cox, *Policing into the 21st Century*, 13 POLICE STUD.: INT’L REV. POLICE DEV. 168, 168 (1990) (highlighting the roles of municipal police that extend beyond law enforcement such as assisting citizens with their private trouble).

65. BRUCE L. BERG, *POLICING IN MODERN SOCIETY* 4 (1999) (discussing the daily work of municipal police, including patrols and emergency services, that closely connects them to the local community). As Gill has observed, “the fundamental goal of the police is order-maintenance, to which end obtaining convictions is only marginally related.” PETER GILL, *POLICING POLITICS* 210–11 (1994). This is the core concept of the constable on patrol (or “cop”)—what Skolnick has called the “peacemaker paradigm.” Skolnick, *supra* note 26, at 192.

66. See JAMES Q. WILSON, *THE INVESTIGATORS* 207 (1978) (providing an example of the conflict between the DEA and the FBI over intelligence-gathering and prosecutorial priorities); Matthew M. Johnson, *FBI’s Intelligence Woes Restir Debate on an American M15*, CQ HOMELAND SECURITY, Oct. 23, 2007, public.cq.com/docs/hs/hsnews110-000002611323.html (discussing the struggle within the FBI to define the appropriate role for its intelligence-gathering function); see also POSNER, *supra* note 15, at 146–47 (describing the challenges facing the FBI’s domestic-intelligence operations); Scott Shane & Lowell Bergman, *F.B.I. Struggling to Reinvent Itself to Fight Terror*, N.Y. TIMES, Oct. 10, 2006, at A1 (“F.B.I. culture still respects door-kicking investigators more than desk-bound analysts sifting through tidbits of data.”).

67. For all that it seems to be the paradigm of a headquarters-driven plot, even the September 11th attacks might have been detected through local counterterrorism. The Hamburg cell—which included Mohammed Atta, Ziad Jarrah, Marwan al Shehhi, and Ramzi Binalshibh—coalesced and became radicalized in the Quds mosque in Hamburg. 9/11 COMMISSION REPORT, *supra* note 63, at

organizing the social world through “clusters” or by heeding the centrality of “nodes,” local intelligence has an important role to play as part of an epistemic federalist arrangement that regards state and local agencies as capable of “seeing” and making sense of phenomena differently from the federal government and sharing a set of methodological and forensic insights into the structure of homegrown terrorism.⁶⁸

B. Intelligence “Coproduction” and Counterradicalization

Not only is local counterterrorism intelligence well positioned to conceptualize aspects of the terror threat—especially the threat posed by homegrown terrorists—it is also situated to play a vital role in gathering the intelligence necessary for understanding the radicalization process. Counterradicalization places demands on intelligence collectors to gather information widely and to adopt the perspective of social anthropologists by attending to the critical interaction between individuals and their social and institutional landscapes.⁶⁹ The intelligence required in order to engage in counterradicalization does not begin and end with known radicals or even those individuals suspected of having already embarked on a path to a radicalized future. Counterradicalization intelligence implies something

160–64. Tyler Drumheller, the retired head of the European Division for the CIA recently commented, “I always believed that the real story of 9/11 was in the notebook of a Hamburg beatcop.” Tyler Drumheller, European Div. Chief, CIA, Panel Discussion at the Center on Law and Security Conference: Intelligence in the Age of National Security (Feb. 1, 2008), *audio available at* <http://www.lawandsecurity.org/podcasts/Intelligence&theLaw.mp3>. The point about the notepad may be an exaggeration—the operational planning for the attacks took place not in Germany but in Afghanistan—but the larger observation about how a local police department might have been best positioned to know about the Hamburg cell’s radicalization is well-taken. See 9/11 COMMISSION REPORT, *supra* note 63, at 156–60 (detailing the planning and preparations that took place in Afghanistan). Drumheller also asserted that the CIA is now authorized to make direct contact with police across Europe as part of their counterterrorism work. Drumheller, *supra*. In other words, even national-level intelligence agencies have come to appreciate that the critical, ground-level information concerning the microgeometry and microgeography of the terrorist threat resides with the local authorities. That this is so suggests another sense in which the local police may have an important role to play in epistemic federalism. Notwithstanding substantial cultural and institutional differences, local police organize the world similarly regardless of the country in which they work and may therefore be well positioned to communicate with one another, employing a common set of cultural norms and a shared professional vocabulary. See, e.g., John P. Sullivan, Global Terrorism and the Police 10 (Mar. 29, 2008) (unpublished manuscript), *available at* http://www.allacademic.com/meta/p_mla_apa_research_citation/2/5/4/3/3/pages254336/p254336-10.php (arguing that national police forces must co-operate with other national police officers across international borders to effectively combat the terrorist threat).

68. Thus, the ODNI decided to train members of an elite new analyst cadre by sending them on a rotation to the NYPD to learn “streetcraft.” Robert K. Ackerman, *Cultural Changes Drive Intelligence Analysis*, SIGNAL ONLINE, May 2007, http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1311&zonedid=31.

69. See SAGEMAN, *supra* note 46, at 24 (“To answer the question ‘How do people become terrorists?’ we need to look at processes, especially the relationships between individuals and their environment.”).

even more far-reaching—namely, an intelligence effort that seeks out knowledge about social facts taking place within discrete communities, including information about individuals believed to be helpful to the authorities in pursuing their counterradicalization agenda.⁷⁰ The British, who have dubbed their equivalent form of counterradicalization intelligence “Rich Picture,” define it generally as the collection of intelligence at local levels to furnish an understanding of the makeup and dynamics of local communities where radicalization could occur and to identify individuals of authority and influence within those communities.⁷¹

Acquiring this sort of broad-gauged intelligence requires resorting to what Elinor Ostrom has referred to as coproduction, “the process through which inputs used to produce a good or service are contributed by individuals” who are “clients” of that public good.⁷² “Coproduction implies that citizens can play an active role in producing public goods and services of consequence to them.”⁷³ There are at least two senses in which the community may participate in coproduced intelligence.⁷⁴ First, local community

70. See *id.* at 71–72 (arguing that, in addition to capturing and eliminating the core group of active terrorists, law enforcement officials must have the requisite knowledge of others that may potentially be connected to terrorist networks).

71. See NEIL HAYNES, METRO. POLICE AUTH., MPS PREVENT DELIVERY STRATEGY (2008), <http://www.mpa.gov.uk/committees/mpa/2008/080724/08/?qu=Rich%20Picture&sc=2&ht=1> (describing Rich Picture as a system utilizing national- and local-level intelligence for counterterrorism via neighborhood policing).

72. Elinor Ostrom, *Crossing the Great Divide: Coproduction, Synergy, and Development*, in STATE-SOCIETY SYNERGY 85, 86 (Peter Evans ed., 1997). Ostrom goes on to explain,

[P]roduction of a service, as contrasted to a good, was difficult without the active participation of those supposedly receiving the service. . . . If citizens do not report suspicious events rapidly to a police department, there is little that department can do to reduce crime in an area or solve the crimes that occur. We developed the term ‘coproduction’ to describe the potential relationships that could exist between the ‘regular’ producer (street-level police officers, school teachers, or health workers) and ‘clients’ who want to be transformed by the service into safer, better educated, or healthier persons. Coproduction is one way that synergy between what a government does and what citizens do can occur.

Id. at 99–100.

73. *Id.* at 86. In discussing coproduction, another commentator has stated,

Co-production is . . . noted by the mix of activities that both public service agents and citizens contribute to the provision of public services. The former are involved as professionals, or ‘regular producers,’ while ‘citizen production’ is based on voluntary efforts of individuals or groups to enhance the quality and/or quantity of the services they receive.

VICTOR A. PESTOFF, A DEMOCRATIC ARCHITECTURE FOR THE WELFARE STATE 160 (2009).

74. There is also a totally different use of the term *coproduction* to mean situations in which local and federal authorities jointly produce intelligence: See, e.g., John P. Sullivan, *The Frontiers of Global Security Intelligence: Analytical Tradecraft and Education as Drivers for Intelligence Reform*, SMALL WARS J., Aug. 22, 2008, <http://www.smallwarsjournal.com/blog/journal/docs-temp/87-sullivan.pdf> (describing the Terrorism Early Warning program pioneered in Los Angeles where local and federal authorities work with private-sector analysts to develop counterterrorism intelligence through open-source intelligence and collaborative analysis).

members may volunteer to serve as covert informants for the police.⁷⁵ Second, and more important considering the scope of the information required, community members and local police may engage in a less formal process of collaborative intelligence work, characteristic of “community policing.”⁷⁶

The centrality of this second kind of coproduced intelligence raises questions about what role federal and local officials should play in these efforts. Of late, the federal government (mainly through the FBI) has become heavily invested in generating counterradicalization intelligence.⁷⁷ The FBI is now authorized under the Attorney General’s Guidelines to engage in this sort of proactive intelligence gathering, divorced from any allegations of criminal wrongdoing.⁷⁸ Furthermore, FBI leadership has made

75. See DAVID SHANZER ET AL., *ANTI-TERROR LESSONS OF MUSLIM-AMERICANS 3* (2010), http://www.sanford.duke.edu/news/Schanzer_Kurzman_Moosa_Anti-Terror_Lessons.pdf (arguing that in order to foster better mutual understanding between law enforcement and Muslim-Americans, “[l]aw enforcement agencies should develop policies on the appropriate use of informants in Muslim-American communities and discuss these policies openly with community leaders” while “Muslim-Americans, for their part, should understand that the use of informants is an accepted, long-standing law enforcement practice and may be necessary in appropriate cases to gather evidence on individuals who are a potential danger”); see also Jacqueline Ross, *Police Informants* (warning that engagement with informants in the criminal context is difficult because “criminal insiders” both provide the best information and have motivations that are most divergent from law enforcement goals), in *PRIVATE SECURITY, PUBLIC ORDER: THE OUTSOURCING OF PUBLIC SERVICES AND ITS LIMITS* 159, 172 (Simon Chesterman & Angelina Fisher eds., 2009).

76. Community policing has been defined as “a philosophy that promotes organizational strategies, which support the systematic use of partnerships and problem-solving techniques, to proactively address the immediate conditions that give rise to public safety issues such as crime, social disorder, and fear of crime.” COPS, U.S. Department of Justice, Community Policing Defined, <http://www.cops.usdoj.gov/default.asp?item=36> (last revised Dec. 15, 2009); see also ALEJANDRO J. BEUTEL, MUSLIM PUB. AFFAIRS COUNCIL, *BUILDING BRIDGES TO STRENGTHEN AMERICA 4* (2009), available at http://www.mpac.org/publications/building-bridges/MPAC-Building-Bridges--Complete_Condensed_Paper.pdf (observing that community policing “gathers and contextualizes various bits of information better to construct a fuller intelligence assessment” (emphasis omitted)). Reliance on the “community” as part of an overall intelligence strategy inevitably raises questions about who represents the community. The answer, clearly, is that no group or institution can lay claim to that sort of representative status. Instead, the community to which I refer is necessarily an artificial construct, comprising mutually opposed elements within a neighborhood or social grouping. Taking this broad view of the community goes some way to ameliorating concerns about public-choice pathologies whereby certain members of the community attempt to gain official sanction for their views.

77. See NATIONAL SECURITY STRATEGY, *supra* note 13, at 19 (“The Federal Government will invest in intelligence to understand this threat and expand community engagement and development programs to empower local communities.”).

78. Under the Attorney General’s Guidelines,

Assessments . . . require an authorized purpose but not any particular factual predication. . . . Likewise, in the exercise of its protective functions, the FBI is not constrained to wait until information is received indicating that a particular event, activity, or facility has drawn the attention of those who would threaten the national security. Rather, the FBI must take the initiative to secure and protect activities and entities whose character may make them attractive targets for terrorism or espionage.

the collection of counterradicalization-related intelligence an organizational priority under the name “domain management.”⁷⁹ But published reports of the FBI’s involvement in this area of intelligence gathering have cast an unflattering light on the Bureau’s activities, which come across as mechanical⁸⁰ or simply bizarre.⁸¹ It is unsurprising perhaps that federal officials, with more attenuated ties to the local community and a substantially smaller footprint, would struggle to furnish intelligence that originates from a combination of covert human sources and a robust network of community voices.

Meanwhile, the local police are in significant respects well positioned to tap into their relationships with the local community to useful effect.⁸² These relationships are a natural fit for local departments that have been practicing a form of community policing for over a generation.⁸³ Not only do these long-term, multifaceted relationships have the effect of potentially restraining the impulses towards overly aggressive counterterrorism measures, they form the backbone of a robust intelligence network. As David Harris has said,

The proactive investigative authority conveyed in assessments is designed for, and may be utilized by the FBI in the discharge of these responsibilities.

OFFICE OF THE ATT’Y GEN., DEP’T OF JUSTICE, ATTORNEY GENERAL’S GUIDELINES FOR DOMESTIC FBI OPERATIONS 17 (2008), available at <http://www.justice.gov/ag/readingroom/guidelines.pdf>.

79. See, e.g., *Intelligence Reform: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 80 (2007) (statement of John S. Pistole, Deputy Director, Federal Bureau of Investigation) (describing the domain management process as a “continuous, systematic approach designed to achieve a comprehensive understanding of a geographic or substantive area of responsibility” that “provides the basis for investigative, intelligence, and management direction by enabling leaders to consider and select courses of action through the knowledge gained, identified gaps in knowledge, and identified gaps in capability”).

80. For example, the FBI has engaged in this discretionary authority to tally the number of mosques in various jurisdictions without delving deeper into the significance of the information being gathered. See Michael Isikoff, *The FBI Says, Count the Mosques*, NEWSWEEK, Feb. 3, 2003, at 6, 6 (noting that the launch of a new FBI initiative includes counting mosques).

81. See Press Release, John Miller, Assistant Dir., Office of Pub. Affairs, Fed. Bureau of Investigation, FBI Response to Congressional Quarterly Article Alleging Willie T. Hulon and Phil Mudd’s Involvement in So-Called “Falafel Investigation” (Nov. 26, 2007), <http://www.fbi.gov/pressrel/pressrel07/editor112607.htm> (denying a story attributing to senior FBI officials a plan to detect Iranian agents by tracking falafel sales in San Francisco grocery stores).

82. The expertise at issue is not, strictly speaking, a matter of familiarity with Islamic theology or legal doctrine. It is closer to an intimate acquaintance with the sociological dimensions of what Olivier Roy has dubbed the “third generation”—meaning the young Muslim men who are themselves frequently the products of parents who sought to assimilate into the cultural mainstream of Western Europe (or, by extension, the United States). OLIVIER ROY, *GLOBALIZED ISLAM* 2 (2004).

83. See BEUTEL, *supra* note 76, at 14 (relating that community-policing practices began in the 1980s); NELSON & BODURIAN, *supra* note 9, at 10 (“[L]ocal officials are intimately connected to the communities—like the Minneapolis Somali one—that global terrorist groups may seek to exploit.”).

“[T]he best—indeed, often the only—source of information on possible terrorist cells on our soil will be Muslim communities themselves.”⁸⁴

C. Problems with Analysis

If local officials are more effective at the bottom-up approach to conceptualizing the threat and at coproducing intelligence, these comparative advantages give out in a number of interconnected areas related to the analysis and the integration of intelligence.⁸⁵ As a leading study of local intelligence has put it, “it is striking how limited the analytic capacity is at the local level.”⁸⁶ First, and most generally, local agencies lack the analytical resources to pull together the disparate data points that are gathered in the name of counterradicalization intelligence and stitch them into a coherent narrative.⁸⁷ Counterradicalization intelligence is, more so than intelligence that is focused on individuals or groups already suspected of involvement in terrorism, especially in need of analysis—otherwise there are merely myriad data points in search of an explanation.⁸⁸ Second, local agencies lack the ability to assess the accuracy of the intelligence they collect—there simply are not mechanisms in place for the vetting of intelligence learned at the local level.⁸⁹ Third, there is no well-established pathway for intelligence learned

84. David A. Harris, *The War on Terror, Local Police, and Immigration Enforcement: A Curious Tale of Police Power in Post-9/11 America*, 38 RUTGERS L.J. 1, 46 (2006); see also Chevigny, *supra* note 7, at 736 (quoting the 1960s vintage National Advisory Commission on Civil Disorders to the effect that police intelligence should use “undercover . . . personnel and informants, but . . . should also draw on community leaders, agencies, and organizations in the ghetto”). More generally, as RAND experts John Arquilla and David Ronfeldt have said, “conflicts may increasingly be waged by ‘networks,’ perhaps more than by ‘hierarchies’ . . . [and] whoever masters the network form stands to gain the advantage.” John Arquilla & David Ronfeldt, *The Advent of Netwar (Revisited)*, in NETWORKS & NETWARS 1, 1 (2001); cf. Chris Wilson, *Searching For Saddam*, SLATE, Feb. 22, 2010, <http://www.slate.com/id/2245228> (exploring how social-networking techniques helped capture Saddam).

85. These analytic shortcomings are themselves related to a lack of funding and a lack of familiarity with the professional norms of the Intelligence Community, especially in the area of analysis. See ROB JOHNSTON, ANALYTIC CULTURE IN THE U.S. INTELLIGENCE COMMUNITY 28–29 (2005) (highlighting the presence of a distinctive culture within the Intelligence Community, especially among analysts).

86. RILEY, *supra* note 24, at 58.

87. See Rascoff, *supra* note 23 (explaining how local law enforcement authorities have become a part of the “domestic intelligence apparatus” but noting that there is an “absence of agencies at the state and local level that are well positioned to understand and cabin the discretion of intelligence officials”). The purpose of this sort of analysis is not to locate the proverbial “needle in the haystack” but to take measure of the haystack itself.

88. This is an example of a troubling phenomenon in intelligence, namely overcollection of intelligence relative to capacity for analysis. See *id.* For a recent example, see Christopher Drew, *Drone Flights Leave Military Awash in Data*, N.Y. TIMES, Jan. 10, 2010, at A1 (describing the inability of the military and government agencies to analyze the flood of data received for intelligence purposes from drone aircraft).

89. See Craig Horowitz, *The NYPD’s War on Terror*, NYMAG, Feb. 3, 2004, http://nymag.com/nymetro/news/features/n_8286/ (quoting Commissioner Ray Kelly’s dismissive comments about the NYPD’s own intelligence capacity prior to his comprehensive reforms: “[T]he

by local agencies to be combined with information learned from other local sources or with federal intelligence to create an integrated threat assessment.⁹⁰ To be valuable to counterterrorism officials, counterradicalization intelligence must be combined with insights learned from other sources and locations—at both the strategic and tactical levels.⁹¹

II. Local Intelligence and Liberty

A. *Informal Mechanisms and Certain Local Strengths*

A small but significant body of scholarship has coalesced around the view that local officials may supply an antidote to concerns about overly aggressive federal counterterrorism measures. Susan Herman⁹² has championed the cause of local counterterrorism in the context of state and local assertions of rights against an aggressive federal government that threatened to commandeer subnational resources. For example, in the aftermath of 9/11, a number of local police officials (notably the Portland, Oregon police chief) resisted FBI efforts to have officers seconded to the Joint Terrorism Task Force.⁹³ Similarly, the Dearborn, Michigan police raised serious concerns about the scope of state participation in federal post-9/11 investigatory activities.⁹⁴ And Mayor Bloomberg of New York City made it clear that local officials would not become engaged in the enforcement of federal immigration laws.⁹⁵ These assertions of local power were informed

NYPD's intelligence division] was an intelligence service in name only. We simply had to get better information. We didn't know what was going on in our own city, let alone the rest of the world.”).

90. I discuss and take critical aim at fledgling attempts by the federal government to harness the power of local intelligence. See *infra* Part III.

91. See RILEY, *supra* note 23, at 58 (asserting that the ideal division of analytical labor would have local authorities taking the general guidance provided by federal officials and applying it to their local domain).

92. Herman was recently tapped to serve as president of the American Civil Liberties Union. American Civil Liberties Union, Susan N. Herman, President of the ACLU, <http://www.aclu.org/leader/susan-n-herman-president-aclu>.

93. See Susan N. Herman, *Collapsing Spheres: Joint Terrorism Task Forces, Federalism, and the War on Terror*, 41 WILLAMETTE L. REV. 941, 942 (2005) [hereinafter Herman, *Collapsing Spheres*] (describing a decision by the Portland City Council to withdraw local officers from JTTF); Susan N. Herman, *Introduction to Our New Federalism? National Authority and Local Autonomy in the War on Terror*, 69 BROOK. L. REV. 1201, 1212–13 (2004) [hereinafter Herman, *National Authority*] (listing various local departments that refused to participate in FBI interviews post-9/11); Tom Lininger, *Federalism and Antiterrorism Investigations*, 17 STAN. L. & POL'Y REV. 391, 393 (2006) (arguing for the use of state bar codes to regulate the conduct of federal government lawyers in antiterrorism prosecutions).

94. See Thacher, *supra* note 40, at 661–62 (“Local [Dearborn] police declined to conduct the interviews themselves, they went to great lengths to explain their participation in a qualified way, and they ultimately adopted the role (at least in part) of monitors for the federal agents and representatives of community concerns.”).

95. See City of N.Y. Exec. Order No. 41 (Sept. 17, 2003) (prohibiting New York City officials from reporting an immigration violation to federal authorities absent evidence of the commission of a separate crime). A similar approach was taken by the International Association of Chiefs of

by a constitutional rationale that was announced by the Supreme Court in a series of cases beginning with *New York v. United States*⁹⁶ and finding its fullest expression in *Printz v. United States*.⁹⁷ Commentators have remarked on how the anticommmandeering logic of *Printz* supplied the justification for these acts of resistance by local police officials⁹⁸ and how the federalism rationale was being invoked opportunistically by political liberals opposed to the Bush Administration's post-9/11 policies.⁹⁹ But the record should not be overinterpreted: these instances of local protest are more revealing of the (inevitably contingent) interest of specific local agencies (or officials) to object to federal policy than of their ability affirmatively to practice intelligence in a manner that is more respectful of rights.

A second, related body of scholarship identifies the presence of a wide range of accountability mechanisms that cause local counterterrorism officials to be more responsive to civil liberties. As Skolnick has written,

New York is a city rich with institutions of accountability, including elections, courts, a vibrant civil liberties and civil rights bar and a free press. Its Mayor and Police Commissioner believe in the rule of law, and are responsive to public opinion. They do not reflexively support their police. With its reorganization post-9/11 to combat terror . . . the New York City Police Department has become something of a model for democratic policing in the U.S. and even around the western world.¹⁰⁰

The observation certainly provides an important perspective, but at the same time, it potentially sidesteps two highly salient facts about intelligence and counterterrorism. First, the secrecy that intelligence entails tends to impede the ability of these civil-society organizations to provide the sort of robust, informal oversight that the police might be subjected to in a more

Police, on the theory that enforcement by local officers of federal immigration laws would interfere on the vital relationships between police and immigrants, including illegal immigrants. Daniel Richman, *The Past, Present, and Future of Violent Crime Federalism*, 34 CRIME & JUST. 377, 411 (2006).

96. 505 U.S. 144 (1992).

97. 521 U.S. 898 (1997).

98. See, e.g., Herman, *National Authority*, *supra* note 93, at 1211 (asserting that while local governments "may not resist or limit federal enforcement efforts within their jurisdictions . . . because of *Printz*, they may not be required to offer their services to help").

99. See Young, *supra* note 25, at 1280 ("[F]ederalism has no dependable liberal or conservative valence as those terms are understood today in an intuitively political sense."); cf. Richman, *supra* note 27 ("To some, the notion of police departments as bulwarks of civil liberties against federal encroachment might sound a bit odd.")

100. Skolnick, *supra* note 26, at 211–12. While Skolnick's observation pertains to New York City, the same logic may apply, with varying degrees of accuracy, to other cities and communities as well.

traditional area of law enforcement activity.¹⁰¹ Second, terrorism issues have proved especially susceptible to cognitive distortion, meaning that arguments from public acquiescence in counterterrorism measures may be overdrawn.¹⁰²

Another scholarly tendency has been to emphasize the relationship of local police officials with the communities they secure, which “move[s] mechanisms of accountability far closer to the public, providing greater ownership and control in terms of how individual communities are policed.”¹⁰³ As Richman has put it,

Local police also play a central role in maintaining order and ensuring public safety, and this gives them a more balanced “portfolio” in dealing with community leaders. The police officer who seeks information from a local Arab-American community leader has probably met and assisted that leader before—protecting his property, ironing out some administrative complexity, or ensuring his safe worship.¹⁰⁴

This balanced portfolio—and the fact that local police are inevitably “repeat players” in the communities in which they operate—does, in fact, create powerful incentives for police officers to negotiate a middle road when it comes to the more intrusive and potentially objectionable aspects of counterterrorism.¹⁰⁵ As a recent empirical study emphasizes, the perception of “procedural fairness” on the part of the (local) police contributes to the willingness of members of the Muslim community to work with authorities in matters of counterterrorism.¹⁰⁶ The federal counterterrorism bureaucracy,

101. Marina Caparini, *Controlling and Overseeing Intelligence Services in Democratic States*, in *DEMOCRATIC CONTROL OF INTELLIGENCE SERVICES* 3 (Hans Born & Marina Caparini eds., 2007).

102. See Cass R. Sunstein, *Terrorism and Probability Neglect*, 26 J. RISK & UNCERTAINTY 121, 133 (2003) (proposing probability neglect, which is especially likely in the context of terrorism, as a partial explanation of public overreaction to highly publicized, low-probability risks).

103. Martin Innes, *Policing Uncertainty: Countering Terror Through Community Intelligence and Democratic Policing*, ANNALS AM. ACAD. POL. & SOC. SCI., May 2006, at 222, 235–36. But see Adrian Vermeule, *Posner on Security and Liberty: Alliance to End Repression v. City of Chicago*, 120 HARV. L. REV. 1251, 1253 (2007) (“[F]or Judge Posner the central consideration in both opinions involved, not federalism or local government, but the scope of civil liberties against any level of government and the scope of executive authority to investigate potential terrorist groups.”). Vermeule takes Judge Posner to mean that there is no upshot for the protection of rights in the national-security arena as between federal and state authority. Whether or not the exegesis is accurate, the insight is overstated. As I maintain, local authorities possess certain advantages in informal governance mechanisms while formal governance is somewhat more assured at the national level. See *infra* subpart II(B).

104. Richman, *supra* note 27.

105. See Thacher, *supra* note 40, at 644 (“The Dearborn case contributes to such study [of authority] by illustrating how surveillance and information-gathering can have chilling effects on a city’s social life that may undermine trust and co-operation with police.”).

106. See Tom R. Tyler et al., *Legitimacy and Deterrence Effects in Counter-Terrorism Policing: A Study of Muslim Americans*, 44 LAW & SOC’Y REV. (forthcoming 2010) (explaining that fair police procedures influence the perceived legitimacy of law enforcement and the willingness of people to co-operate with them).

meanwhile, interacts with the community in a manner that is typically more one-off, meaning that it does not have a structural incentive to strike a balance in favor of rights protection.¹⁰⁷ At the same time, it is hard to know whether this logic dictates local restraint in the more elusive (and less overt) aspects of intelligence collection that, at least in theory, are likely to remain unknown to community members.

Other potential liberty benefits of practicing counterterrorism intelligence at the local level are worth mentioning. First, local agencies, more so than federal, have the ability to reallocate resources to various missions flexibly, as a function of a dynamic perception of the relative benefits and costs (including opportunity costs) of regulating the threat.¹⁰⁸ Unlike Washington agencies, whose regulatory mandates often outlive their missions, a local agency (especially an inevitably cash-strapped local police department with a wide range of institutional responsibilities) typically cannot afford to throw money at a problem that is of diminishing importance.¹⁰⁹ This flexibility helps to avoid one of the core threats to liberty of domestic intelligence—the tendency of intelligence programs, over time, to outlive their strategic missions and to become enmeshed in surveillance of activities or persons unconnected to addressing any urgent security problem.¹¹⁰

A final sense in which local intelligence officials—with their heightened reliance on partnerships with members of the community—may be more attentive to staying within constitutional boundaries relates to the First Amendment's religion clauses. Counterradicalization necessarily

107. The Department of Homeland Security's Office of Civil Rights and Civil Liberties has initiated dialogue on issues of radicalization, but thus far the program only covers approximately five communities across the country. VIOLENT ISLAMIST EXTREMISM, *supra* note 52, at 15. And while each of the FBI's fifty-six field offices has a Community Relations Unit, these units do not focus on issues of radicalization or, for that matter, terrorism. *Id.*

108. See Jon M. Peha, *Fundamental Reform in Public Safety Communications Policy*, 59 FED. COMM. L.J. 517, 523 (2007) ("The advantages of local control are that local decisionmakers are able to match local resources (e.g., tax dollars) to the most pressing local needs.").

109. See, e.g., David Johnston, *With Crime Up, a City's Police Force Questions the Focus on Terror*, N.Y. TIMES, July 24, 2008, at A17 (reporting that the homeland security and terrorism-related focus of federal resources and grants is limiting local law enforcement in its ability to fight community crime effectively).

110. The recent abuse of national security letters by the FBI supplies a good example of the dangers of this kind of "mission creep." See, e.g., David Stout, *F.B.I. Head Admits Mistakes in Use of Security Act*, N.Y. TIMES, Mar. 10, 2007, at A1 (describing Congress's outraged response to reports that the FBI had used national security letters to improperly obtain personal information and business records). While it is true that local departments may want to stress their vulnerability to terrorism in order to compete for federal funding, it does not necessarily follow that the departments will actually devote resources to the issue once the cash is on hand. Cf. Johnston, *supra* note 109 (reporting that local law enforcement officers would prefer more discretion in the use and allocation of federal resources to fight crime).

entails engagement with Islamic culture and theology.¹¹¹ Unlike officials who practice intelligence in this area,¹¹² nongovernmental coproducers of intelligence do not run the risk of transgressing the dictates of the First Amendment by sanctioning a moderate version of Islam.¹¹³

B. *Formal Governance and Local Vulnerabilities*

Yet, for all that local counterterrorism officials have been celebrated as “offer[ing] the best premise of appropriately tempered zeal” in the post-9/11

111. See REWRITING THE NARRATIVE, *supra* note 12, at 13–20 (recommending a comprehensive approach involving a number of strategic, functional, and organizational steps to counter radical Islamist extremism).

112. The First Amendment runs only against governmental actors. Of central importance is the Establishment Clause as it functions to create “‘a wall of separation between Church and State.’” *Everson v. Bd. of Educ.*, 330 U.S. 1, 16 (1947) (quoting *Reynolds v. United States*, 98 U.S. 145, 164 (1878)). Establishment Clause jurisprudence is famously knotty, but has generally moved in the direction of greater tolerance for governmental endorsement of religion in society. See, e.g., *Elk Grove Unified Sch. Dist. v. Newdow*, 542 U.S. 1, 35 (2004) (O’Connor, J., concurring in judgment) (“The Court has permitted government, in some instances, to refer to or commemorate religion in public life.”). However much latitude the government may have to support religion in general, the deep engagement with Islam entailed by counterradicalization would seem to implicate precisely the “excessive government entanglement with religion” that has been consistently prohibited. *Lemon v. Kurtzman*, 403 U.S. 602, 613 (1971); see also *McCreary County v. ACLU*, 545 U.S. 844, 881 (2005) (refusing to permit the display of the Ten Commandments in a county courthouse because the display had a “predominantly religious purpose”); *Agostini v. Felton*, 521 U.S. 203, 233 (1997) (“Not all entanglements, of course, have the effect of advancing or inhibiting religion. . . . Entanglement must be ‘excessive’ before it runs afoul of the Establishment Clause.”). A recent policy paper advocates community, rather than law enforcement, involvement in counterradicalization, although seemingly for reasons of effectiveness rather than compliance with the Bill of Rights. See BEUTEL, *supra* note 76, at 16 (“Law enforcement must focus its energies on counterterrorism (i.e., criminal activities), not counterradicalization. . . . The role Muslim communities should play is in counterradicalization efforts through better religious education, social programs and long-term constructive political engagement.”).

113. President Obama has followed the pervasive federal practice of framing engagement with Islam as promoting “tolerance” and discouraging “extremism.” In his speech at Cairo University, Obama invoked both concepts, asserting that “America is not—and never will be—at war with Islam. We will, however, relentlessly confront violent extremists who pose a grave threat to our security.” Barack Obama, U.S. President, Remarks by the President on a New Beginning (June 9, 2009), available at http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-at-Cairo-University-6-04-09. Later in the speech, Obama began his discussion of religious freedom by noting that “Islam has a proud tradition of tolerance” before urging his audience to work to close the “fault lines” between Sunni and Shiites. *Id.* Whether governmental actors actually sidestep religious engagement by framing their normative account of Islam in these terms is an open question. See Yvonne Yazbeck Haddad & Tyler Golson, *Overhauling Islam: Representation, Construction, and Cooption of “Moderate Islam” in Western Europe*, 49 J. CHURCH & ST. 487, 511–12 (2007) (describing two interventionist policies that Western European governments have converged on in attempting to establish a new Islam: institutionalizing representative Muslim bodies and facilitating the construction of Muslim spaces); Robert Lambert, *Salafi and Islamist Londoners: Stigmatised Minority Faith Communities Countering al-Qaida*, 50 CRIME L. & SOC. CHANGE 73, 82–83 (2008) (discussing the effects of the British government’s Sufi Muslim Council’s description of two groups of U.K. Muslims, the Salafi and Islamist communities, as dangerous extremists, and openly siding with their religious opponents); Samuel J. Rascoff, *Establishing “Official Islam”* (June 2010) (unpublished manuscript, on file with author).

period,¹¹⁴ significant concerns remain, especially pertaining to the intelligence mission. As local police become more and more involved in “true” intelligence work, the adequacy of informal mechanisms and community relationships to supply sufficient governance becomes doubtful.¹¹⁵ A generation ago, formal governance of local intelligence agencies was supplied by consent decrees overseen by federal courts.¹¹⁶ But these consent decrees no longer effectively cabin police authority, and the internal guidelines that were promulgated to give them effect have similarly been relaxed.¹¹⁷ As a local police respondent to a RAND survey commented in explaining his department’s intelligence governance, “Issues are simply talked about as they come up.”¹¹⁸ Nor do legislative checks on executive action generally have teeth at the local level.¹¹⁹ And judicial review is notoriously unavailable in intelligence matters, owing to the convergence of

114. Richman, *supra* note 27.

115. Although my emphasis here is on the absence of formal governance mechanisms, it bears mentioning that a crucial informal tool is also missing from the local-intelligence-governance repertoire, namely historical consciousness. While measurement of historical awareness within an organization is inevitably difficult, it seems intuitively correct that practitioners of domestic intelligence at the federal level are more keenly aware of the excesses of the J. Edgar Hoover Era than local police are acquainted with the checkered history of Red Squads. To be certain, modern policing has become highly professionalized over the last generation, but that professionalization has typically come in areas of core crime fighting through modalities that allow management by numbers, such as the NYPD’s COMPSTAT program. I thank Kenji Yoshino for raising this provocative idea.

116. See Chevigny, *supra* note 7, at 747–68 (discussing consent decrees resolving federal civil rights litigation in New York City, Chicago, and Memphis).

117. See *Handschu v. Special Serv. Div.*, 605 F. Supp. 1384, 1417 (S.D.N.Y. 1985) (approving a consent decree for the NYPD in the context of investigations of political groups); see also Steigman, *supra* note 7, at 765–70 (detailing litigation in September 2002 in which the *Handschu* consent decree was modified by judicial order). But see RILEY, *supra* note 23, at 34 (noting the ways in which various local intelligence agencies have supplemented oversight by reference to external governance bodies); Raymond W. Kelly, The 2006 Paul Miller Distinguished Lecture: Safeguarding Citizens and Civil Liberties (Nov. 15, 2006) (discussing an external legal advisory board for NYPD intelligence, chaired by a distinguished member of the bar), in 59 RUTGERS L. REV. 555, 557–58 (2007).

118. RILEY, *supra* note 23, at 33.

119. For example, the New York City Council Public Safety Committee has never held a hearing about the oversight component of the NYPD Intelligence Division, which is funded entirely by private foundations. Pincus, *supra* note 16. As Committee Chair Peter Vallone Jr. put it, “The City Council does not have any real expertise in that area to conduct meaningful oversight. Perhaps some other system needs to be established.” He went on to argue, “We should have oversight. That is what our forefathers envisioned when they came up with checks and balances. There is no way to perform an effective check if we weren’t actually aware of what is happening.” *Id.* Of course, it is also true the congressional intelligence committees have fallen short in providing a robust check on Executive action. See Rascoff, *supra* note 8 (noting that intelligence gathering at the subnational level has largely gone ungoverned). See generally Anne Joseph O’Connell, *Intelligent Oversight* (calling for more centralized congressional oversight over intelligence activities and stating that even after 9/11, intelligence committees complained that they were not receiving necessary information from Executive agencies), in *THE IMPACT OF 9/11 AND THE NEW LEGAL LANDSCAPE* 161–64 (Matthew Morgan ed., 2009).

a host of pragmatic and doctrinal limits of federal jurisdiction.¹²⁰ In sum, local intelligence increasingly operates in a formal governance vacuum.¹²¹

III. Institutional Design

A. Existing Arrangements

The purpose of a co-operative federalist arrangement ought to be to leverage the strengths of the local actors in counterterrorism intelligence while addressing their vulnerabilities—particularly their worrisome lack of analytic capacity and formal governance mechanisms. And yet, these objectives have been effectively missing from the federal government's post-9/11 attempts to harness the power of state and local counterterrorism agencies.¹²² The FBI, DHS, and ODNI have each attempted to combine efforts with state and local officials through separate top-down institutional arrangements. Intending to draw upon the expertise and manpower of local law enforcement,¹²³ the FBI has spearheaded JTTFs,¹²⁴ DHS underwrites Fusion Centers,¹²⁵ and the ODNI (and its constituent agency, the NCTC) has begun to play a more prominent role in serving as an analytic resource for subnational-counterterrorism-intelligence practitioners.¹²⁶ All three programs are flawed.¹²⁷

120. See Rascoff, *supra* note 8 (describing how the role of judges in the governance of intelligence is limited).

121. See David A. Harris, *Law Enforcement and Intelligence Gathering in Muslim and Immigrant Communities After 9/11*, 34 N.Y.U. REV. L. & SOC. CHANGE (forthcoming 2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1330023 (suggesting that law enforcement and Muslim communities jointly negotiate limitations to the use of informants for counterterrorism intelligence gathering).

122. The first JTTF dates back to 1980, but the program was very substantially increased after 9/11. Press Release, Fed. Bureau of Investigation, Protecting America Against Terrorist Attack: A Closer Look at the FBI's Joint Terrorism Task Forces (Dec. 1, 2004), <http://www.fbi.gov/page2/dec04/jtff120114.htm>.

123. NYPD Deputy Commissioner Falkenrath has said, "The federal government, while well intentioned, has no overarching vision for terrorism-related information sharing with state and local agencies and no federal direction or leadership. . . . At least three Cabinet-level officers . . . have substantial oversight responsibility for the federal government's information-sharing system; none of them appears truly engaged by the topic." Falkenrath, *Hearing*, *supra* note 43, at 20.

124. Federal Bureau of Investigation, *supra* note 35.

125. Department of Homeland Security, *supra* note 36.

126. Interagency Threat Assessment and Coordination Group, *supra* note 37. As Greg Treverton, an experienced student of domestic intelligence, recently put it,

[T]hree different agencies seemed to have responsibility for intelligence connections with state and local officials after the 2004 Act [creating the Director of National Intelligence]: the DHS, which had the congressional mandate; the FBI, which had the troops in the field through its field offices and JTTFs; and the ODNI, which had the stake.

GREGORY F. TREVERTON, INTELLIGENCE FOR AN AGE OF TERROR 114 (2009).

127. Judge Posner acknowledges that neither the DHS nor the FBI model of reaching out to local officials is adequate, but believes that an MI5-like organization would do better. As he explains,

1. *JTTFs and Co-option.*—The JTTF approach—as it concerns local officials¹²⁸—is essentially one of co-option. While ostensibly designed to facilitate greater communication across jurisdictional lines and to leverage the know-how and manpower of local police forces,¹²⁹ JTTFs have tended instead to undermine the benefits of robust counterterrorism federalism by co-opting state and local officials (as well as a raft of federal officials from agencies outside the FBI) and subordinating them to FBI managers and their national agenda.¹³⁰ Although local participation on certain JTTFs may be robust—well over one hundred NYPD detectives serve on the New York JTTF, for example—in many others it is sparse, with only a handful of detectives participating in offices that are otherwise dominated by FBI special agents.¹³¹ Regardless of the absolute size of the local cohort, local officials on JTTFs are functionally federalized: they are given access to classified information and are discouraged from reaching back into their home agencies.¹³² More generally, they are also cut off from the ground-up

MI5 has been able to do what the FBI and the Department of Homeland Security have been unable to do—integrate local police into the national domestic intelligence system. It is a vital mission. Local police, border patrol, customs officers, and private security and intelligence personnel gather enormous masses of information at the source, as it were. They are well positioned to notice anomalies that may be clues to terrorist plotting. We need an agency that will integrate local police and other information gatherers into a comprehensive national intelligence network, as MI5 has done in Britain.

POSNER, *supra* note 15, at 155–56.

128. JTTFs are not designed solely to achieve collaboration between federal and subfederal actors; much of the “joint-ness” achieved by JTTFs is a function of co-operation within the federal government. Cf. Brig Barker & Steve Fowler, *The FBI Joint Terrorism Task Force Officer*, FBI L. ENFORCEMENT BULL., Nov. 2008, at 12, 13 (reporting that 24% of personnel within JTTFs are from state and local law enforcement agencies and that 17% are from non-FBI federal agencies).

129. See Robert A. Martin, *The Joint Terrorism Task Force: A Concept That Works*, FBI L. ENFORCEMENT BULL., Mar. 1999, at 23, 25 (observing that the NYPD brings insights to a JTTF that come from years of living and working with New Yorkers); Federal Bureau of Investigation, *supra* note 37 (indicating that a primary benefit of a JTTF is intelligence sharing across agencies).

130. See, e.g., Herman, *Collapsing Spheres*, *supra* note 93, at 951–53 (discussing the degree to which the terms of the JTTF agreement between the FBI and the City of Portland, Oregon, led to problematic federal control of local police officers).

131. For example, the Dearborn, Michigan police department contributes a single officer to the local JTTF. Thacher, *supra* note 40, at 665. See generally Barker & Fowler, *supra* note 128, at 13 (reporting that 24% of personnel within JTTFs are from state and local law enforcement agencies and that 17% are from non-FBI federal agencies).

132. Local politicians (including the mayor of Dearborn) emphasize that they have no dealings with the officer assigned to the JTTF to underscore that at the local level, they are not involved in the gathering of intelligence. See Barker & Fowler, *supra* note 128, at 13 (“Mayor Guido, for example, emphasized the city’s hands-off relationship with the officer who serves as their primary liaison to the task force . . .”). As one commentator has put it, “the city maintains considerable distance between [the officer dedicated to the JTTF] and the rest of city government, as if to insulate itself from the contaminating effects of offender search activities. *Id.* at 666. Although there are some 100 JTTFs around the country, Press Release, *supra* note 122, many of them have their own

methodology that is characteristic of local police work and gives local officers a natural advantage over federal agents at the sort of intelligence gathering that is necessary for counteracting contemporary threats.¹³³ Furthermore, and of clear significance, local officials deployed to JTTFs are not explicitly made part of the FBI's domain management initiatives, the Bureau's core domestic-intelligence program by which it attempts to "achieve a comprehensive understanding of a geographic or substantive area . . . to better arm our leadership with strategic domain knowledge to proactively identify and neutralize national security and criminal threats."¹³⁴

2. *Fusion Centers and (Misguided) Devolution.*—Fusion Centers are theoretically more promising because they have typically been initiated by state and local agencies and feature a more significant state and local presence.¹³⁵ But as several recent studies point out, the "devolution" model they have pursued has proved disappointing in practice.¹³⁶ First, Fusion Centers have rapidly been transformed into organizations that tackle "all threats [and] all hazards"¹³⁷—meaning that the counterterrorism intelligence

branches dedicated to monitoring foreign areas of responsibility such as the Horn of Africa, Saudi Arabia, and Iraq. Guy Lawson, *The Fear Factory*, ROLLING STONE, Feb. 2008, at 60–65. This global approach flies in the face of the ground-up counterterrorism intelligence gathering practiced by local police and is unnecessary given the availability of sound intelligence on these areas coming out of the core intelligence agencies headquartered in Washington, D.C. For a recent critical assessment of the work of the JTTFs, see Lawson, *supra*.

133. See *supra* subpart I(A).

134. *Intelligence Reform: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 80 (2007) (statement of John S. Pistole, Deputy Director, Fed. Bureau of Investigation).

135. See MICHAEL GERMAN & JAY STANLEY, AM. CIVIL LIBERTIES UNION, WHAT'S WRONG WITH FUSION CENTERS? 6 (2007), available at http://www.aclu.org/pdfs/privacy/fusioncenter_20071212.pdf ("Intelligence fusion centers grew in popularity among state and local law enforcement officers as they sought to establish a role in defending homeland security by developing their own intelligence capabilities. These centers evolved largely independently of one another . . . and were individually tailored to meet local and regional needs."). As of 2009, there were seventy-two Fusion Centers nationwide. Department of Homeland Security, State and Local Fusion Centers, http://www.dhs.gov/files/programs/gc_1156877184684.shtm (last modified Sept. 16, 2009).

136. One commentator recently noted,

[I]t is widely accepted that effective intelligence processes are essential in terrorism prevention, and that state, local, and tribal law enforcement and other public sector agencies are in a unique position to play a role in this process. There is agreement that as the majority of critical infrastructure sites in the country are owned and/or operated by the private sector, that it too has an important role to play. However, the uneven, grassroots development of fusion centers, devoid of strong federal direction and national consensus on their mission, scope, and 'ownership' threatens the value of their contribution and increases the risk of abuse.

Siobhan O'Neil, *The Relationship Between the Private Sector and Fusion Centers: Potential Causes for Concern and Realities*, HOMELAND SECURITY AFF., Apr. 2008 (Supp. 2), at 3–4.

137. Ryan Singel, *Feds Tout New Domestic Intelligence Centers*, WIRED, Mar. 20, 2008, <http://www.wired.com/threatlevel/2008/03/feds-tout-new-d>; see also U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-35 HOMELAND SECURITY: FEDERAL EFFORTS ARE HELPING TO ALLEVIATE SOME CHALLENGES ENCOUNTERED BY STATE AND LOCAL FUSION CENTERS 5 (2007) ("The

mission has become one among many. Even when they do address terrorism, Fusion Centers have devolved the wrong function from the center to the periphery: information exchange (fusion) rather than information collection and analysis.¹³⁸ To be certain, information sharing is a *sine qua non* of an effective co-operative federalist approach to counterterrorism intelligence. But information sharing presupposes the existence of intelligence that has already been acquired and properly analyzed—goals that are not themselves advanced by Fusion Centers.¹³⁹ DHS has recently sought to provide more centralized control of the Fusion Centers and to develop “mechanisms, in coordination with federal, state, local, tribal, and territorial authorities, to improve the capability of state and major urban area fusion centers to gather, assess, analyze and share locally generated and national information and intelligence, in order to provide complete pictures of regional and national threats and trends.”¹⁴⁰ But it remains unclear how DHS will make good on these aspirations.¹⁴¹

majority [of the centers] had missions and scopes of operations that included more than just counterterrorism-related activities, such as collecting, analyzing, and disseminating criminal as well as terrorism-related information.”).

138. See Zoe Baird, *Why Information Sharing Is Not Always Enough*, FED. COMPUTER WK., Feb. 17, 2010, <http://fcw.com/articles/2010/02/22/comment-zoe-baird-markle-national-security.aspx> (“The job isn’t done when information is shared but rather when it is thoroughly analyzed by people not only collecting the dots but also connecting them.”). That Fusion Centers are distributed evenly across the states suggests another flaw: that the widely disparate vulnerabilities that states face vis-à-vis terrorism have not been accounted for. Cf. Eric Lipton, *Homeland Security Grants to New York Slashed*, N.Y. TIMES, May 31, 2006, at A1 (detailing how security grants were cut for cities such as New York City and Washington D.C. while cities such as Omaha and Louisville “got a surge of new dollars”).

139. Cf. DEP’T. OF JUSTICE & DEP’T OF HOMELAND SEC., FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION AND INTELLIGENCE IN A NEW WORLD 2 (2005), available at <http://www.fas.org/irp/agency/ise/guidelines.pdf> (“The concept of fusion has emerged as the fundamental process to facilitate the sharing of homeland security-related and crime-related information and intelligence. For purposes of this initiative, fusion refers to the overarching process of managing the flow of information and intelligence across levels and sectors of government.”). Other DHS- and FBI-led initiatives in counterradicalization-focused outreach have also proved unsuccessful at combining federal and state strengths. See VIOLENT ISLAMIST EXTREMISM, *supra* note 52, at 15 (observing that “the efforts by [DHS Office of Civil Rights and Civil Liberties] and the FBI’s Community Relations Unit are not tied into programs administered by local police departments, some of which are quite comprehensive”).

140. *I&A Reconceived: Defining a Homeland Security Intelligence Role: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 111th Cong. (2009) (statement of Bart R. Johnson, Acting Under Secretary for Intelligence and Analysis, Department of Homeland Security), available at <http://homeland.house.gov/siteDocuments/20090924104844-11233.pdf>; see also *id.* (“Central to this proposal is the establishment, at the Secretary’s direction, of a new Joint Fusion Center Program Management Office”). The Department of Defense has also recently sought to share more intelligence with subnational entities via the Fusion Centers. Press Release, Dept. of Def., DOD Announces New Information-Sharing Access to Help Fusion Centers Combat Terrorism (Sept. 14, 2009), <http://www.defense.gov/Releases/Release.aspx?ReleaseID=12974>.

141. Nevertheless, Fusion Centers remain part of the contemporary institutional landscape. See NATIONAL SECURITY STRATEGY, *supra* note 13, at 20 (“To prevent acts of terrorism on American

3. *ITACG and Consumption.*—The ODNI’s experiment—while still largely untested¹⁴²—is potentially more promising than either the FBI or the DHS models. Indeed, it might have been awareness of this fact that prompted the White House and Congress recently to expand the authority of the ODNI—and specifically the NCTC—in co-operative federalism.¹⁴³ The NCTC has begun to provide a conduit for members of the subfederal law enforcement community to gain access to classified information through the still-fledgling ITACG.¹⁴⁴ The Group brings together representatives of state, local, and tribal officers alongside national experts to expose the former to federal intelligence and the latter to the distinctive counterterrorism issues that arise at the subnational level.¹⁴⁵ The NCTC is well suited to hosting the

soil . . . [w]e will continue to integrate and leverage state and major urban area fusion centers that have the capability to share classified information . . .”).

142. See PROGRAM MANAGER, INFO. SHARING ENV’T, REPORT ON THE INTERAGENCY THREAT ASSESSMENT AND COORDINATION GROUP: SECOND REPORT FOR THE CONGRESS OF THE UNITED STATES, THE SECRETARY OF HOMELAND SECURITY, AND THE DIRECTOR OF NATIONAL INTELLIGENCE 17 (2009) [hereinafter PROGRAM MANAGER REPORT] available at http://www.ise.gov/docs/ITACG_Status_Report_PM_ISE_FINAL_24Nov09.pdf, (demonstrating the difficulty of evaluating the program at such an early stage); *id.* at 20 (listing the names of the six state and local law enforcement and emergency personnel currently assigned to the ITACG Detail).

143. See *Homeland Security Intelligence at a Crossroads: The Office of Intelligence & Analysis’ Vision for 2008: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong. (2008) (statement of Rep. Jane Harman, Chairwoman, Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment), available at <http://homeland.house.gov/SiteDocuments/20080227111045-34957.pdf> (pronouncing that ITACG will remain and expand despite resistance by other agencies). In her prepared statement before the February 26, 2008, hearing, Chairwoman Harman castigated veteran CIA official Charlie Allen, who runs DHS’s Intelligence and Analysis office. “Bottom line, Charlie: you are not effectively serving the State and [local officials] who are the people who will prevent the next attack.” *Id.*

144. The Group began as part of WHITE HOUSE, NATIONAL STRATEGY FOR INFORMATION SHARING 18 (2007), available at http://georgewbush-whitehouse.archives.gov/nsc/infosharing/NSIS_book.pdf, and was more recently signed into law as part of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, sec. 521, § 210D, 121 Stat. 266, 328–32 (to be codified at 6 U.S.C. § 124k). The Group consists of a Detail and an Advisory Group. *Id.* § 210D(b). The purpose of the Detail is to “integrat[e], analyz[e], and assist[] in the dissemination of federally-coordinated information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, through appropriate channels identified by the ITACG Advisory Council.” *Id.* § 210D(b)(2).

145. *Id.*; see also WHITE HOUSE, *supra* note 144, at 18–19 (discussing the purposes of creating the ITACG). It was located in the NCTC over the vigorous objection of DHS, which sought a monopoly over counterterrorism information sharing with state and local entities. At a February 26, 2008, hearing of the House of Representatives Homeland Security Committee’s Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, Chairwoman Jane Harman noted that she had “a major issue with [DHS’s] endless refusal to take the ITACG seriously and to build a robust State, local, and tribal presence at the NCTC that makes the intelligence production process for State and locals better.” *Homeland Security Intelligence at a Crossroads*, *supra* note 143. The key word here is “production”—which signifies a role for the local entity in producing intelligence, not merely in consuming it. The NYPD has actually dispatched an officer to sit among the federal

Group because it is has genuine analytic expertise in the area of counterterrorism and enjoys a statutory mandate to devise overall U.S. counterterrorism strategy.¹⁴⁶ This initiative represents a welcome break from past practice in which local officials were regularly prevented from gaining access to classified threat information, even if the threats at issue carried security implications for the jurisdiction of the local officials from whom the information was being withheld.¹⁴⁷ Still, the NCTC initiative perpetuates the flawed habit of regarding subnational participants principally as consumers of federal intelligence products, rather than as representatives of agencies with the capacity to gather and analyze intelligence alongside federal counterparts. Thus, a recently issued annual report notes that the “goal of the ITACG Detail is to further enable the production of clear, tailored, relevant, official federally-coordinated threat information in a timely, consistent and usable manner” for the benefit of subnational actors.¹⁴⁸ The local officials are relegated to identifying potentially useful information from within federal intelligence databases and advising federal officials about tailoring analytic products to suit the distinctive needs and capacities of subnational intelligence consumers.¹⁴⁹

B. *Toward Homegrown Counterterrorism*

What would a properly conceived set of co-operative federalist arrangements look like in the area of counterterrorism intelligence? Three ingredients are essential. First, there ought to be robust local intelligence capacity overseen through a process of centralized “regulatory” review simultaneously aimed at providing more rights-compliant and more

officials at NCTC (not through ITACG). Tina Moore, *U.S. Snoops Get NYPD Lift to Sniff Out Qaeda*, N.Y. DAILY NEWS, Mar. 26, 2008, at 8.

146. 50 U.S.C. § 404o(d) (2006); see also RICHARD A. BEST JR., CONG. RESEARCH SERV., THE NATIONAL COUNTERTERRORISM CENTER (NCTC)—RESPONSIBILITIES AND POTENTIAL CONGRESSIONAL CONCERNS 4 (2010) (referring to the current NCTC charter which includes providing “strategic operational plans for military and civilian counterterrorism efforts and for effective integration of counterterrorism intelligence and operations across agency boundaries within and outside the US”).

147. See, e.g., Edward J. Tully & E.L. Willoughby, *Terrorism: The Role of Local and State Agencies*, NAT’L EXECUTIVE INST. ASSOCIATES ET AL., May 2002, <http://www.neiassociates.org/state-local.htm> (criticizing federal law enforcement and intelligence attitudes towards local and state agencies as the principal flaw in their ability to combat terroristic threats).

148. PROGRAM MANAGER REPORT, *supra* note 142, at 5.

149. See *id.* at 10 (detailing the daily operations of the ITACG Detail (made up of state, local, and tribal (SLT) personnel), including “assist[ing] in identifying time-sensitive terrorism threats to locations within the United States” and “identif[y]ing suitable strategic and foundational assessments as candidates for downgrading or tailoring for dissemination to SLT and private sector consumers”).

analytically rigorous intelligence.¹⁵⁰ The kind of review I have in mind, rooted in ideas of rationality¹⁵¹ and modeled generally on the role of the Office of Information and Regulatory Affairs (OIRA) within the regulatory state,¹⁵² would help plug the governance vacuum in which local intelligence currently operates. A federal overseer (potentially housed within ODNI or DHS) would help calibrate the degree to which specific local intelligence agencies could undertake certain programs of intelligence gathering and help define their scope.¹⁵³ Would such intelligence gathering be likely to yield timely and important intelligence? Or perhaps local intelligence resources would be more usefully devoted to another area or problem? For example, in the current threat environment in which there is substantial concern about radicalization within the Somali-American community,¹⁵⁴ federal regulators could help enlist local officials in cities with large concentrations of Somali-Americans like Minneapolis¹⁵⁵ or Lewiston, Maine,¹⁵⁶ to employ their human networks to collect relevant counterradicalization intelligence. Federal officials would also help to determine whether certain collection modalities would be likely to transgress basic norms, especially when viewed in the light of their (potentially modest) comparative intelligence payoffs.

A prerequisite for such a governance mechanism, of course, both as a constitutional and as a practical matter, is willing local participation,¹⁵⁷ which gets to the second pillar of the regime I am contemplating. Federal funding and know-how are needed to ensure the viability of local intelligence programs. The requirement of federal funding speaks for itself. But the need for sophisticated training in intelligence work is equally vital. Training must span all aspects of the job from the finer points of human intelligence collection (especially given the imperatives of intelligence coproduction discussed above) to intelligence analysis to the legal environment in which domestic

150. As I have argued elsewhere, these goals are mutually reinforcing. See Rascoff, *supra* note 8 (“Not only does rationality review pave the way for more accurate and more rights-protective intelligence, it also lays the methodological foundation for a more coordinated and consistent intelligence process, and one with more robust and centralized accountability mechanisms.”).

151. I use the term “rationality” in an expansive sense, to embrace ideas of cost-benefit analysis and cost effectiveness, as well as more explicitly normative judgments. *Id.*

152. See The White House, Office of Management and Budget, Information and Regulatory Affairs, http://www.whitehouse.gov/omb/infoREG_default/ (“OIRA carries out several important functions, including reducing paperwork burdens, reviewing Federal regulations, and overseeing policies relating to privacy, information quality, and statistical programs.”).

153. For an extensive discussion on the potential for regulatory oversight of intelligence, see Rascoff, *supra* note 8.

154. See, e.g., Andrea Elliott, *A Call to Jihad, Answered in America*, N.Y. TIMES, July 12, 2009, at A1 (chronicling the rise of young ethnically Somali jihadists in Minneapolis).

155. *Id.*

156. See Jesse Ellison, *The Refugees Who Saved Lewiston*, NEWSWEEK, Jan. 17, 2009, at 69 (describing the recent influx of Somali refugees into Lewiston, Maine).

157. See Michael A. Sheehan, Op-Ed., *The Terrorist Next Door*, N.Y. TIMES, May 4, 2010, at A31 (arguing that concerns about the potential financial and political costs have caused local departments to be leery of covert intelligence gathering).

intelligence operates and the civil liberties concerns that are uniquely implicated by a domestic intelligence apparatus. While there may be certain affinities between law enforcement and intelligence work, the two domains remain quite distinct.

Third, the federal government must create and maintain a virtual intelligence network available to local agencies, especially to major metropolitan police departments.¹⁵⁸ Through participation in the network, locals would be able to “push” intelligence out to other local agencies¹⁵⁹ or to Washington, and to receive timely information from the national Intelligence Community. Best practices could also be shared, as could hard-won lessons in intelligence failures.¹⁶⁰

IV. Conclusion

A decade and a half ago Stewart Baker posed the question whether our spies should be cops.¹⁶¹ In view of the advent of homegrown terrorism and the government’s commitment to counterradicalization, today’s dilemma is the reverse: should our cops be spies? If, as a strong bipartisan constituency has already signaled,¹⁶² the answer to that question is yes, the first task becomes achieving conceptual clarity about what role local officials ought to play as part of an overall intelligence strategy that conjoins elements of national and subnational authority to practice “intelligence under law.”¹⁶³ In this Article I have begun to do just that, emphasizing areas of comparative local strength as well as vulnerability, and suggesting what a rightly conceived set of institutional arrangements ought to look like. Conceptual work of this sort is a necessary foundation for homegrown counterterrorism to play a significant role in addressing homegrown terrorism.

158. Cf. NATIONAL SECURITY STRATEGY, *supra* note 13, at 20 (“We are improving information sharing and cooperation by linking networks to facilitate Federal, state, and local capabilities to seamlessly exchange messages and information . . .”).

159. Local intelligence collaboration is a vital piece of the puzzle. An example is supplied by the NYPD’s Operation Sentry, which brings together members of police departments throughout the extended New York City Metropolitan area. See Press Release, NYPD, NYPD Convenes Operation Sentry Members for Annual Conference (May 5, 2009), http://www.nyc.gov/html/nypd/html/pr/pr_2009_ph10.shtml.

160. The creation of a non-Washington-centric Information Sharing Environment in which “[a]ll players in th[e] network—including those at the edges—would be able to create and share actionable and relevant information” has been vigorously advocated by the Markle Foundation as early as 2003. TASK FORCE ON NAT’L SEC. IN THE INFO. AGE, MARKLE FOUND., CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY 8 (2003). As of yet, nothing approaching that framework has been implemented.

161. Stewart A. Baker, *Should Spies Be Cops?*, FOREIGN POL’Y, Winter 1994–1995, at 36.

162. See *supra* Part III.

163. See James B. Comey, *Intelligence Under the Law*, 10 GREEN BAG 2D 439, 443–44 (2007) (“We know that there may be agonizing collisions between our duty to protect and our duty to that constitution and the rule of law. . . . [I]n the long-run, intelligence under law is the only sustainable intelligence in this country.”).

Choosing Both: Making Technology Choices at the Intersections of Privacy and Security

Alexander W. Joel*

Advanced technology and its creative application remain a comparative advantage for the United States, but we fear that the Intelligence Community is not adequately leveraging this advantage And this problem affects not only intelligence collection; we also lag in the use of technologies to support analysis.¹

It's six minutes before midnight as a surveillance society draws near in the United States. With a flood of powerful new technologies that expand the potential for centralized monitoring . . . we confront the possibility of a dark future where our every move, our every transaction, our every communication is recorded, compiled, and stored away, ready for access by the authorities whenever they want.²

[T]he [Intelligence Community] must *exemplify America's values*: operating under the rule of law, consistent with Americans' expectations for protection of privacy and civil liberties, respectful of human rights, and in a manner that retains the trust of the American people.³

["Buridan's ass"]: a paradox whereby a hungry and thirsty donkey, placed between a bundle of hay and a pail of water, would die of hunger and thirst because there was no reason for him to choose one resource over the other.⁴

When you come to a fork in the road, take it.⁵

Technology plays a critical role in intelligence activities, enabling intelligence agencies to pursue their national-security mission more effectively and efficiently. The United States has long been a leader in

* Alexander Joel is the Civil Liberties Protection Officer for the Office of the Director of National Intelligence (ODNI). The views expressed in this Article are his own and do not imply endorsement by the ODNI or any other U.S. government agency.

1. COMM. ON THE INTELLIGENCE CAPABILITIES OF THE U.S. REGARDING WEAPONS OF MASS DESTRUCTION, REPORT TO THE PRESIDENT OF THE UNITED STATES 326 (2005), available at http://www.gpoaccess.gov/wmd/pdf/full_wmd_report.pdf.

2. AM. CIVIL LIBERTIES UNION, EVEN BIGGER, EVEN WEAKER: THE EMERGING SURVEILLANCE SOCIETY: WHERE ARE WE NOW? 4 (2007), http://www.aclu.org/files/pdfs/privacy/bigger_weaker.pdf.

3. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, THE NATIONAL INTELLIGENCE STRATEGY 2 (2009), available at http://www.dni.gov/reports/2009_NIS.pdf.

4. THE OXFORD DICTIONARY OF PHRASE AND FABLE 180 (Elizabeth Knowles ed., 2006), available at <http://www.encyclopedia.com/doc/1O214-Buridansass.html>.

5. YOGI BERRA, THE YOGI BOOK: "I REALLY DIDN'T SAY EVERYTHING I SAID!" 48 (1998).

technological innovation,⁶ and the Intelligence Community⁷ (IC) has recognized the importance of leveraging American technological advantages.⁸ Calls for the IC to make better use of technology are not uncommon, nor are complaints about its failure to capitalize on the latest technological developments;⁹ this is particularly true following news of a major event that the IC did not anticipate.¹⁰ Such calls often raise concurrent concerns about the civil liberties and privacy implications of placing powerful new capabilities in the hands of intelligence operatives, where they might be used in potentially unanticipated ways, cloaked from public scrutiny by rules that protect “sources and methods” from disclosure.¹¹

Intelligence officers and policy makers standing at the intersection of security and privacy can find themselves presented with a conundrum: how to make prudent technology choices? Moving in one direction seems imperative for accomplishing important national-security missions, yet raises red flags about potential impacts on privacy and civil liberties. Moving in another direction seems necessary to protect civil liberties, yet raises alarms about potentially dangerous security gaps. This dilemma calls up the image of Buridan’s ass, caught between two competing and compelling

6. EDMUND B. FITZGERALD, *GLOBALIZING CUSTOMER SOLUTIONS: THE ENLIGHTENED CONFLUENCE OF TECHNOLOGY, INNOVATION, TRADE, AND INVESTMENT* 23 (2000).

7. The term “Intelligence Community” is defined in § 3(4) of the National Security Act of 1947, 61 Stat. 495 (codified as amended at 50 U.S.C. § 401(a) (2006)), in relatively general terms. The specific members of the IC are listed in the Director of National Intelligence’s guide. NATIONAL INTELLIGENCE: A CONSUMER’S GUIDE 9 (2009), available at http://www.dni.gov/IC_Consumers_Guide_2009.pdf. There are seventeen elements of the IC: Office of the Director of National Intelligence; Central Intelligence Agency; National Security Agency; Defense Intelligence Agency; Federal Bureau of Investigation National Security Branch; National Reconnaissance Office; National Geospatial-Intelligence Agency; Drug Enforcement Administration, Office of National Security Intelligence; Department of Energy Office of Intelligence and Counterintelligence; Department of Homeland Security Office of Intelligence and Analysis; Department of State Bureau of Intelligence and Research; Department of Treasury Office of Intelligence and Analysis; Air Force Intelligence; Army Intelligence; Coast Guard Intelligence; Marine Corps Intelligence; and Naval Intelligence. *Id.*

8. See Michael N. Schmitt, *The Principle of Discrimination in 21st Century Warfare*, 2 YALE HUM. RTS. & DEV. L.J. 143, 153 (1999) (asserting that developed states leverage their technological advantages in areas such as information management).

9. See, e.g., AMY B. ZEGART, *SPYING BLIND: THE CIA, THE FBI, AND THE ORIGINS OF 9/11* 137 (2007) (noting how inefficiently the FBI adopted new technology, including FBI Director Louis Freeh removing his computer from his office in 2000 for lack of use).

10. Indeed, soon after the attempted attack on December 25, 2009, on Flight 253, the White House announced that “[t]he U.S. government had sufficient information to have uncovered and potentially disrupted the December 25 attack . . . but analysts . . . failed to connect the dots that could have identified and warned of the specific threat . . . Information technology . . . did not sufficiently enable the correlation of data that would have enabled analysts to highlight the relevant threat information.” Press Release, White House, White House Review Summary Regarding 12/25/2009 Attempted Terrorist Attack (Jan. 7, 2010), <http://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack>.

11. See, e.g., Martin E. Halstuk & Eric B. Easton, *Of Secrets and Spies: Strengthening the Public’s Right to Know About the CIA*, 17 STAN. L. & POL’Y REV. 353, 354–56 (2006) (asserting that after *CIA v. Sims*, 471 U.S. 159 (1985), the CIA has been shielded from public scrutiny).

considerations.¹² It also brings to mind Yogi Berra's famous advice on encountering a fork in the road: when forced to choose between security and privacy, find ways to "take it"—to have it both ways.¹³ Through it all, intelligence agencies must remember this: protecting privacy and civil liberties is not optional. The question they face is not *whether* to provide such protections—agencies are obligated, by law and duty, to provide them. Rather, the question is *how* to provide them while accomplishing the intelligence mission.

I. The Broader Context

The paradoxical directive that the IC use technology more aggressively because of its potential to make agencies more effective at their missions (which includes, of course, "spying"), yet refrain from using technology because of its potential intrusiveness, is a recurring one. Concerns that authorities for "espionage" might be abused if not properly overseen, given the advent of new capabilities, find eloquent expression in Justice Louis Brandeis's dissent in a 1928 Supreme Court case. In discussing wiretapping and the invention of the telephone, Justice Brandeis warned:

Subtler and more far-reaching means of invading privacy have become available to the Government The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.¹⁴

Fifty years later, the Church Committee echoed Justice Brandeis's concerns, warning that at a time when "the technological capability of Government relentlessly increases, we must be wary about the drift toward 'big brother government.' The potential for abuse is awesome and requires special attention to fashioning restraints which not only cure past problems but anticipate and prevent the future misuse of technology."¹⁵ Privacy and civil liberties advocacy groups, academic commentators, and others have similarly raised such concerns over the years.¹⁶

12. See *supra* note 4 and accompanying text.

13. See *supra* note 5 and accompanying text.

14. *Olmstead v. United States*, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting).

15. S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES OF THE UNITED STATES SENATE, S. REP. NO. 94-755, at 276 (1976).

16. See *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. (2010) (statement of James X. Dempsey, Center for Democracy and Technology), available at <http://www.judiciary.house.gov/hearings/pdf/Dempsey100505.pdf> ("[I]t is clear that the balance among . . . the individual's right to privacy, the government's need for tools to conduct investigations, and the interest of service providers in clarity and customer trust . . . has been lost as

Public discourse is complicated in the IC arena by information disclosure restrictions and inhibitions that have traditionally gone hand-in-hand with intelligence activities.¹⁷ In part due to this lack of public transparency, popular imagination, as reflected in and fueled by fiction, television, and movies, is free to take leaps in different directions, uninhibited by the constraints—legal, policy, technical, operational, budgetary, and cultural—under which intelligence agencies operate. Satellites that peer around corners, analysts who can instantaneously access data from any source by tapping on a laptop, watch centers that can redirect surveillance cameras at any point on the globe to follow an individual running through a crowded square, supercomputers that can contact someone on his cell phone and then send him a message on an electronic billboard—these are the capabilities commonly portrayed in books and movies. Even while knowing that creative imaginations are at work, commentators focus on the imagery emerging from these works for the insights they may provide into potential intelligence capabilities, and concomitantly, potential abuses.¹⁸

Whether fact or fiction, such imagery can affect public perceptions, and thus expectations, of the IC's capabilities. Some may wonder whether agencies could deploy technology to instantaneously and precisely detect, identify, and track a terrorist before an attack.¹⁹ To achieve that capability, should the government acquire more computing power, access more data, and deploy more surveillance equipment? This vision of a technologically enabled future obscures bothersome details about technology that do not

powerful new technologies create and store more and more information about our daily lives"); Neil M. Richards, *Intellectual Privacy*, 87 TEXAS L. REV. 387, 394 (2008) (arguing that courts should use the First Amendment to protect the people from the government).

17. See 50 U.S.C. § 403-1 (2006) (directing the Director of National Intelligence to protect intelligence sources and methods from unauthorized disclosure); *CIA v. Sims*, 471 U.S. 159, 177 (1985) (upholding the CIA's decision to withhold its sources and methods from a disclosure request under the Freedom of Information Act).

18. For example, *EAGLE EYE* (DreamWorks Pictures 2008), directed by D.J. Caruso, is about a secret Department of Defense computer system that uses its ability to both access and control nearly all networked computers and devices to surveil and direct the actions of an ordinary American. A leading advocacy organization noted that "beneath the fast-paced, action packed plot are looming questions about the future of technology and the importance of government accountability." ELEC. PRIVACY INFO. CTR., EPIC ALERT, June 22, 2009, http://epic.org/alert/EPIC_Alert_16.12.html. Similarly, *ENEMY OF THE STATE* (Touchstone Pictures 1998), directed by Tony Scott, about a rogue cell within the National Security Agency (NSA) that uses NSA's surveillance technology to track every move and conversation of an American (portrayed by Will Smith), leading him at one point to disrobe to avoid surveillance, has been cited in discussions about domestic surveillance. See, e.g., Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy Under the USA PATRIOT Act*, 80 DENV. U. L. REV. 375, 376 n.7 (2002) (noting the Orwellian themes of the movie).

19. See, e.g., 24 (Fox Broadcasting Co. 2001) (portraying government agencies as using a variety of sophisticated technology to identify suspects, prevent terrorism, and apprehend criminals); *MINORITY REPORT* (Twentieth Century Fox & Dreamworks Pictures 2002) (telling the story of a world in which technology allows police to see the future and arrest potential offenders before the "precrimes" are committed).

always get comparable screen time.²⁰ Technology functions imperfectly resulting in the potential for error. Moreover, as technology enables access to more data, it increases demands on human analysts to review and act on that data. Thus, even without considering the ways in which fiction writers have imagined that the government could abuse such technologies, we should be concerned with the less dramatic aspects of these technology-enabled visions, such as false positives and increased “noise” in the system.²¹

Conversely, fictional imagery of the IC’s technological prowess may cause others to fear that such powerful capabilities could be abused or misused and to question how these types of capabilities could ever be properly controlled.²² Is the answer simply to prevent intelligence agencies from using advanced technological capabilities so as to minimize the risk of an Orwellian future? Or would there be consequences to outright prohibitions, affecting how well intelligence agencies can perform their authorized missions?

These contrasting visions of technology’s promise and peril may play a role in the paradoxical signals sent to the IC: do both more and less with technology. As the Church Committee put it thirty years ago in the midst of documenting what it characterized as a “massive record of intelligence abuses”:

We must acknowledge that the assignment which the Government has given to the Intelligence Community has, in many ways, been impossible to fulfill. It has been expected to predict or prevent every crisis, respond immediately with information on any question, act to meet all threats, and anticipate the special needs of Presidents. And then it is chastised for its zeal.²³

20. See, e.g., NAT’L COMM’N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 88 (2004) (describing problems of technology development including its cost, tendency to fail, and use by terrorists for their own purposes, but concluding that in spite of all of this “Americans’ love affair with [technology] leads them to also regard it as the solution”).

21. See, e.g., *Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs Before the S. Judiciary Comm.*, 110th Cong. 12 (2007) (statement of Kim Taipale, Executive Director, Center for Advanced Studies in Science and Technology Policy) (discussing false positives in data mining); ROBERTA WOHLSTETTER, PEARL HARBOR: WARNING AND DECISION (1962) (discussing the failure to anticipate the Japanese attack on Pearl Harbor as a failure to identify “signals” from the “noise,” with “signal” meaning a sign of an enemy move, and “noise” meaning competing signals that are useless for predicting that move).

22. See, e.g., JAY STANLEY & BARRY STEINHARDT, AM. CIVIL LIBERTIES UNION, BIGGER MONSTER, WEAKER CHAINS 1–3 (2003), available at http://www.aclu.org/files/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf (using George Orwell’s writings and the movie *Minority Report* to illustrate the real-world pervasiveness of surveillance systems and the fact that such systems “rarely remain confined to their original purpose”).

23. S. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES OF THE UNITED STATES SENATE, S. REP. NO. 94-755, at 290 (1976).

II. Keeping the Scale Balanced

Faced with these competing considerations, the obvious way ahead is to strike a balance: capitalize on America's technological prowess while protecting privacy and civil liberties through safeguards and oversight. Even the use of the term "balance," however, presents difficulties, returning us to the imagery of either/or choices. It raises the specter of a government official using a scale to make a decision about whether to deploy a program, where the official metaphorically weighs the benefits for national security that a new technology has to offer against the costs to privacy or civil liberties that using the technology might entail. In this vision, if the security benefits outweigh the liberty costs, the official approves the program. Alternatively, if there are only slight security benefits but heavy liberty costs, the official disapproves the program. Inherently, this view assumes a tradeoff between security and liberty—what weighs down one side of the scale necessarily causes the other side to go up—with no compromise options.²⁴

This is a limited and ultimately unhelpful use of the balance metaphor. While it is true that there are tensions between security and liberty interests, forcing either/or choices is neither helpful to practitioners nor realistic. In practice, programs are frequently adjusted to address concerns during successive review and approval stages. And protecting privacy and civil liberties is not optional; the question is not "whether," but "how." Thus, rather than imagining using a scale to weigh security interests *against* liberty interests in forcing an either/or choice to approve a new technological capability, consider viewing the scale as a means to determine the "weight" that is needed on each side to *keep the scale balanced between security and liberty*. Our focus should be not on which side outweighs the other to inform a go/no-go decision. It should be on giving *equal weight* to security and liberty interests affected by the technology so that the scale *remains balanced*.²⁵

On the security side of the scale, imagine that a new program will add weight to the scale with aspects that are potentially intrusive on privacy or that impact civil liberties.²⁶ We should examine the program to determine

24. When appearing on a PBS Frontline special, a former FBI counterterrorism official stated, I can give you more security, but I've got to take away some rights. And so there's a balance. Personally, I want to live in a country where you have a common-sense, fair balance because I'm worried about people that are untrained, unsupervised, doing things with good intentions that at the end of the day, harm our liberties.

Frontline: Spying on the Home Front (PBS television broadcast May 15, 2007), available at <http://www.pbs.org/wgbh/pages/frontline/homefront/etc/script.html>.

25. Since program personnel are already focused on the security benefits of the new technology, the net effect of this approach is to provide a methodology for addressing the civil liberties implications of that technology under which those implications are on at least an equal footing with security interests. Of course, if there are legal requirements that apply, those must be followed regardless.

26. For purposes of this use of the balance metaphor, the scale only measures security/liberty interests that are in tension with one another, and thus only records weight on the security side of the scale if a technology program's security measures intrude on liberty interests. The more

whether the degree of intrusiveness occasioned through use of technology is legally authorized, necessary, and narrowly tailored toward achieving a legitimate security purpose. We should also ask whether there is a less intrusive way of achieving the same purpose. The effect of these inquiries is to find ways to add only as much weight to this side of the scale as is necessary and appropriate to achieve legitimate security purposes. On the liberty side of the scale, our inquiry should focus on determining whether and how to add weights in the form of safeguards and oversight to counterbalance the impacts of the added weight on the security side. Certain technologies, then, could add weight to the security side, such as surveillance technologies, while others could add weight to the liberty side—such as anonymization and auditing applications.²⁷

III. Protections for the Liberty Side of the Scale

Of course, this approach to the balance metaphor in evaluating new uses of technology is only helpful if there are effective privacy and civil liberties protections from which to draw to counterbalance any potential new challenges. Public discussion regarding the sources of such protections tends to focus on the Constitution—typically the First and Fourth Amendments—and statutes such as the Foreign Intelligence Surveillance Act of 1978²⁸ (FISA), the Electronic Communications Privacy Act,²⁹ and the Privacy Act of 1974.³⁰ However, the IC operates within an infrastructure for protecting privacy and civil liberties, for which the Constitution and applicable laws lay only the foundation.³¹

Beyond this foundation, the IC conducts its activities under the Executive Branch framework established by Executive Order 12,333.³² It

intrusive the program, the more it weighs down the security side of the scale; a nonintrusive program would add no weight to the scale.

27. The idea of weighing considerations in a manner that avoids a zero-sum decision-making approach has been put forward by others as well. For example, Amitai Etzioni, in *The Limits of Privacy*, discusses four criteria for determining whether privacy concerns and the common good are in balance: Is there a well-documented, macroscopic threat to the common good, not merely a hypothetical threat? Can the threat be countered by non-privacy-intrusive measures? Can the threat be countered by minimally intrusive measures? If privacy-intrusive measures are needed, are there safeguards and measures to address “undesirable side effects”? AMITAI ETZIONI, *THE LIMITS OF PRIVACY* 12–14 (1999).

28. Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered titles of U.S.C.).

29. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

30. 5 U.S.C. § 552a (2006).

31. Indeed, all government employees, including intelligence officers, take an oath to support and defend the Constitution, as required by statute. 5 U.S.C. § 3331 (2006). Note that Article VI of the Constitution requires that all “executive and judicial Officers, both of the United States and of the several States, shall be bound by Oath or Affirmation, to support this Constitution.” U.S. CONST. art. VI, cl. 3.

32. Exec. Order No. 12,333, 3 C.F.R. 200 (1982), as amended by Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004),

begins by directing that “[a]ll reasonable and *lawful* means must be used to ensure that the United States will receive the best intelligence possible,”³³ and makes clear that “[a]ll means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used.”³⁴ The Order goes on to provide, “The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.”³⁵

Part 1 then identifies the roles and responsibilities of the national-security and intelligence elements of the Executive Branch. Part 2 enumerates restrictions on the conduct of intelligence activities.³⁶ Section 2.3 governs how IC elements may handle information concerning U.S. persons.³⁷ It provides that:

[IC elements] are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director.³⁸

As further protection, those procedures, some of which are classified, go into extensive detail about what IC elements can do with respect to such information.³⁹ Section 2.3 additionally provides that “[t]hose procedures

Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008), *reprinted as amended* in 50 U.S.C. § 401 (2006).

33. *Id.* (emphasis added).

34. *Id.* § 1.1(a). The Order defines “United States person” broadly, as “a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.” *Id.* § 3.5(k).

35. *Id.* § 1.1(b).

36. Part 3 defines terminology. Note that the Order was revised significantly in 2008 to align it with the Intelligence Reform and Terrorism Act of 2004. *See* Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008) (citing the Intelligence Reform and Terrorism Act of 2004 as a source of authority for updating Exec. Order No. 12,333, which included striking and replacing the entirety of Part 1).

37. Exec. Order No. 12,333 § 2.3.

38. *Id.*

39. The procedures for the Department of Defense’s intelligence elements and those of the FBI are unclassified. *See* DEP’T OF DEF., DIRECTIVE 5240.1-R, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (1982) [hereinafter DOD DIRECTIVE], available at <http://www.js.pentagon.mil/whs/directives/corres/pdf/524001r.pdf>; OFFICE OF THE ATT’Y GEN., U.S. DEP’T OF JUSTICE, THE ATTORNEY GENERAL’S GUIDELINES FOR DOMESTIC FBI OPERATIONS (2008), available at <http://www.justice.gov/ag/readingroom/guidelines.pdf>. The FBI has released its comprehensive

shall permit collection, retention, and dissemination of the following types of information,” and lists specific types, including “information that is publicly available,” “information constituting foreign intelligence or counterintelligence,” “information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation,” “information acquired by overhead reconnaissance not directed at specific United States persons,” and “incidentally obtained information that may indicate involvement in activities that may violate Federal, state, local, or foreign laws.”⁴⁰

Thus, it is not enough for IC elements to satisfy requirements imposed by the Constitution or applicable statutes when collecting, retaining, and disseminating information concerning U.S. persons. They must also ensure that their actions are consistent with Executive Order 12,333 and the implementing procedures. For example, an IC element’s procedures may require it to review lawfully collected information concerning a U.S. person within a certain time period after collection to determine whether it is “information constituting foreign intelligence or counterintelligence” or whether it meets other collection and retention criteria under the Executive Order.⁴¹ If information fails to meet such criteria, the agency’s procedures may require the agency to destroy the information or transfer it (with no copies retained) to another agency that has proper authority.⁴² These rules are interpreted and applied by agency Offices of General Counsel and by the Department of Justice, and are audited and overseen by agency Offices of Inspector General.⁴³ Possible violations are reported to the Intelligence Oversight Board of the President’s Intelligence Advisory Board.⁴⁴

In addition to Executive Branch protections, there are protections from the other branches as well. For example, the FISA Court issues and enforces orders relating to activities under FISA jurisdiction. Congress conducts

internal guidance under the Attorney General’s guidelines, FBI Domestic Investigations and Operations Guide, which are available at <http://foia.fbi.gov/foiaindex/diog.htm>.

40. Exec. Order No. 12,333 § 2.3.

41. *Id.*

42. *See, e.g.,* DOD DIRECTIVE, *supra* note 39, at 20–21 (describing procedures for retention of information about U.S. persons). Note also that section 2.3 of Executive Order 12,333 authorizes IC elements to collect, retain, and disseminate information concerning U.S. persons “consistent with the authorities provided by Part 1 of this Order.” Even if information is “publicly available,” under section 2.3(a) of the Order, the collection, retention, and dissemination of that information must be “consistent with the authorities” of that IC element. Intelligence officials must always be mindful of tying their activities to their authorized mission, even when dealing with information that is available to the public at large. This point becomes particularly relevant in considering the implications of technological change.

43. Exec. Order No. 12,333 § 1.6.

44. Exec. Order No. 13,462, 73 Fed. Reg. 11,805 (Mar. 4, 2008), *as amended by* Exec. Order No. 13,516, 74 Fed. Reg. 56,521 (Nov. 2, 2009). Section 1.6(c) of Executive Order 12,333 requires IC elements to report to the Intelligence Oversight Board “intelligence activities of their elements that they have reason to believe may be unlawful or contrary to executive order or presidential directive.”

oversight as a co-equal branch of government.⁴⁵ Congressional oversight is a fundamentally important element of the civil liberties and legal infrastructure for the Intelligence Community, since Congress has access to classified information and can therefore assess the propriety of IC programs and exercise its constitutional prerogatives with respect to such activities, including the power of the purse.⁴⁶

And there are new entities involved in providing privacy and civil liberties advice and oversight in the post-9/11 era, including the DNI's Civil Liberties Protection Officer,⁴⁷ the Privacy and Civil Liberties Oversight Board,⁴⁸ and Privacy and Civil Liberties Officers established under the Implementing Recommendations of the 9/11 Commission Act of 2007.⁴⁹ Nongovernmental organizations also play an important role by providing focused attention, expertise, and advocacy on the intersection of technology, privacy, and national security.

IV. Responding to Technological Change: Can Liberty Keep Up?

The importance of this infrastructure of laws, rules, and oversight extends beyond serving as a source from which to draw protections to

45. Congress oversees and authorizes intelligence activities through the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence and appropriates funds for such activities through appropriations committees. Due to the diversity of the community (various elements are nested within other departments, and activities impact areas of concern to multiple committees), various other committees of Congress are also involved in reviewing intelligence activities. Section 502 of the National Security Act of 1947 requires that congressional intelligence committees be kept "fully and currently informed" of all intelligence activities (covert action is covered under section 503), "with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources or methods and other exceptionally sensitive matters." 50 U.S.C. § 413(a) (2006). Moreover, section 501 of that Act requires the President to ensure any "illegal intelligence activity is reported promptly to the intelligence committees." *Id.*

46. While Congress has historically played a role in overseeing intelligence activities since the founding of the nation, the current system of intelligence oversight was explicitly established following the Church Committee era, to work in conjunction with legislation such as FISA and with Executive Branch measures such as Executive Order 12,333 and its predecessors. See RICHARD A. POSNER, UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM 195 (2006); Loch K. Johnson, *Governing in the Absence of Angels* (detailing the relatively few times since the 1970s when Congress has devoted significant attention to reforming oversight of the IC), in WHO'S WATCHING THE SPIES 57, 60 (Hans Born et al. eds., 2005).

47. The National Security Act states,

[T]he Civil Liberties Protection Officer shall ensure that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures . . . implemented by the . . . elements of the intelligence community . . . and ensure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information.

National Security Act of 1947, 50 U.S.C. § 403-3d(b).

48. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 109-13, § 1061, 118 Stat. 3638, 3684 (codified at 5 U.S.C. § 601 (2006)).

49. Implementing Recommendations of 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 801, 121 Stat. 266, 352 (to be codified at 42 U.S.C. § 2000ee).

counterbalance the impact of new capabilities being considered by the IC. Intelligence officers act on—and react to—the world around them, which is changing at ever-increasing rates due to technology.⁵⁰ Staggering amounts of communications and data course through the world's telecommunications systems and databases, with processing capabilities being added to smaller and smaller devices (themselves networked in new and innovative ways).⁵¹ Consumers now have at their fingertips impressive capabilities to access and process data from public or commercial sources. Seemingly simple query tools—coupled with the profusion of content made available by users, providers, and publishers on the Internet—provides the average computer user access to information that was unimaginable when certain of the IC-related rules just described were originally written.

The explosion of information that the average consumer has access to today—which is also accessible to the average terrorist—has implications for protections on the liberty side of the scale. Rules written with particular technologies in mind, for example, might now be seen to impede intelligence activities in ways that were not originally contemplated; they might be portrayed as weighing down the liberty side in a manner that unduly restricts intelligence capabilities. For example, in supporting the successive FISA amendments (the Protect America Act in 2007⁵² and the FISA Amendments Act in 2008⁵³) government officials stated that proposed amendments were needed to modernize FISA's provisions.⁵⁴ Conversely, concerns might also be raised that, because technological changes have made so much information available from so many sources, the existing rules are no longer weighty enough to adequately restrict intelligence capabilities in the manner originally intended. For example, commentators have pointed out that the growing amount of data about people's personal lives now processed and stored by third parties is not protected by the Fourth Amendment (sometimes referred to as the "third party doctrine").⁵⁵

50. See, e.g., John F. Duffy, *Inventing Invention: A Case Study of Legal Innovation*, 86 TEXAS L. REV. 1, 66 (2007) (asserting that the electronics and software industries particularly have seen "highly rapid" technological change in the last quarter century).

51. See, e.g., JUNE JAMRICH PARSONS & DAN OJA, NEW PERSPECTIVES ON COMPUTER CONCEPTS 304 (2010 ed.) ("[T]he Internet is huge. Although exact figures cannot be determined, it is estimated that the Internet handles more than an exabyte of data every day. An exabyte is 1.074 billion gigabytes, and that's a nearly unimaginable amount of data.").

52. Pub. L. No. 110-55, 121 Stat. 552 (to be codified at 50 U.S.C. §§ 1803, 1805a-1805c).

53. Pub. L. No. 110-261, 122 Stat. 2436 (to be codified in scattered sections of 50 U.S.C.).

54. See, e.g., *Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 19 (2007) (statement of J. Michael McConnell, Director of National Intelligence) ("Communications technology has evolved in ways that have had unforeseen consequences under FISA. Technological changes have brought within FISA's scope communications that the IC believes the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the Act.").

55. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1137-38 (2002) ("[I]t is only recently that we are truly beginning to see the profound implications of the Court's third party doctrine Government information gathering

When confronted with changes in technology that seemingly outpace anything originally contemplated, what should practitioners do? It may be illuminating to briefly reconsider *Olmstead v. United States*⁵⁶ in this context. In that 1928 case, the government used warrantless surveillance to track a “conspiracy of amazing magnitude” involving a network that included financiers, scouts, drivers, and even an attorney.⁵⁷ The surveillance worked: the FBI disrupted the plot. On appeal, the Supreme Court confronted the question of how to apply an “old rule”—the Fourth Amendment’s requirements⁵⁸ with its references to “persons, houses, papers, and effects”—to a “new tool,” wiretapping of telephone wires. The Court upheld the surveillance as legal,⁵⁹ reasoning that “the invention of the telephone . . . and its application for the purpose of extending communications” could not justify expanding the Fourth Amendment “to include telephone wires, reaching to the whole world from the defendant’s house or office.”⁶⁰ In doing so, the Court declined invitations to extend the principles of the Fourth Amendment by analogy to the “invention of the telephone,” rejecting, for example, the analogy of postal mail.⁶¹ Instead, the Court deferred to Congress to address the broader implications of government wiretapping.⁶²

Of course, *Olmstead* is best known for Justice Louis Brandeis’s eloquent dissent. In contrast to the majority, Justice Brandeis found that, just as the Court had previously “sustained the exercise of power by Congress . . . over objects of which the fathers could not have dreamed,” clauses guaranteeing individual protection must also “have a similar capacity of adaptation to a changing world.”⁶³ Justice Brandeis reasoned that “[t]ime works changes [and] brings into existence new conditions and purposes. Therefore a principle to be vital must be capable of wider application than the mischief which gave it birth.”⁶⁴ Justice Brandeis did not believe that a new constitutional amendment, or legislative action, was called for to address the Fourth

from the extensive dossiers being assembled with modern computer technology poses one of the most significant threats to privacy of our times.”).

56. 277 U.S. 438 (1928).

57. *Id.* at 455.

58. The Fourth Amendment provides,

The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

59. *Olmstead*, 277 U.S. at 464–65.

60. *Id.* at 465.

61. *Id.*

62. *Id.* at 465–66.

63. *Id.* at 472.

64. *Id.* at 472–73 (Brandeis, J., dissenting) (quoting *Weems v. United States*, 217 U.S. 349, 373 (1910)).

Amendment's use of terms such as "papers" and "effects."⁶⁵ Rather, he reasoned by analogy and found that "[t]here is, in essence, no difference between the sealed letter and the private phone message."⁶⁶

What is the lesson for us? For intelligence professionals facing a landscape where new telephone-type inventions seem to multiply at an ever-increasing rate, pressure may be brought to bear to make a sharp break from prior rules—even technology-neutral ones—and to write new rules for a new era and address changes in technology that were not contemplated when the original rules were developed, particularly where those rules are oriented toward outdated technologies. Perhaps, like the *Olmstead* majority,⁶⁷ we should accept that, for certain new developments, the old rules do not apply and policy makers must develop new ones.

However, when existing rules are based on sound, technology-neutral principles that protect privacy and civil liberties while enabling agencies to pursue their mission, it is not clear that writing new ones will leave us in a better place, even if those who originally crafted the rules did not imagine what technology enables today. Rules can and should be harmonized, clarified, and updated. Where wholesale revision is called for to address technological change, the challenge will be this: technology is complex, difficult to understand and describe, and continues to change rapidly. It is, therefore, a daunting task to pose to lawyers, policy makers, and the rule-making process to capture the essence of technology's implications—in all its richness—and in a way that will enable its effective use while addressing civil liberties implications.

A visualization exercise illustrates the problem. The rate at which technology changes over time can be depicted on a chart as a steep, diagonal line, to show that it changes rapidly.⁶⁸ Indeed, the line might also be jagged, to illustrate how technology can leap ahead in sudden spurts. By contrast, the line showing the rate at which government policies change, be they laws or internal government regulations, would be more horizontal, with periodic step increases to show that policy changes gradually and predictably.⁶⁹ The two lines probably would not intersect—notwithstanding the title of this

65. *Id.*

66. *Id.* at 475. Indeed, he found wiretapping more problematic, since it involved the communications of more people. *Id.* at 476.

67. *Id.* at 465–66.

68. See *supra* note 50 and accompanying text.

69. See, e.g., Ivan K. Fong, *Law and New Technology: The Virtues of Muddling Through*, 19 YALE L. & POL'Y REV. 443, 454–56 (2001) (describing courts throughout the twentieth century as "struggling to fit new technologies" into then-existing legal concepts); Bradley C. Karkkainen, *Bottlenecks and Baselines: Tackling Information Deficits in Environmental Regulation*, 86 TEXAS L. REV. 1409, 1414 (2008) (reporting that innovative industrial sectors often complain that technology-based regulations are obsolete once promulgated because the industry has moved on to new production technologies).

symposium—leaving a gap between policy and technology at any given point in time.

This exercise illustrates a fairly obvious truth: by the time the lawyers, technologists, privacy officers, and policy makers agree on a new policy to address a technological change, that technology may well have changed again.⁷⁰ If the goal is to update rules to keep pace with such change, the process may be a never-ending one. More specifically, since technologists and lawyers speak different languages, there is a risk of “technical translation error,” that the new policy will get the technology wrong.⁷¹ In addition, it is quite possible that the new policy will use terminology, or assumptions, specific to a particular technology and therefore will quickly become outdated.⁷²

Referring again to the imaginary chart, since it shows a steep line with technology changing quickly and a shallow line with policies changing gradually, we can predict that policies will perpetually lag technologies, leaving a gap. How to fill it? Proceeding without rules is not an option; privacy and civil liberties must be protected. Waiting to deploy the technology while new rules are written (standing there like Buridan’s ass) is no more attractive.

It may be prudent to consider Justice Brandeis’s approach:⁷³ to find the underlying principles animating the existing rules, to reason by analogy,⁷⁴ and to find ways to apply those principles to the new conditions created by technological change (akin to our common law tradition). This can help fill policy gaps while also informing policy makers as they develop new rules, should they determine such rules are called for. Applying these principles to

70. I am referring to policies that require acts of Congress or formal departmental or interagency processes to implement, rather than policies that could be implemented at the operating level.

71. See, e.g., Robert P. Merges, *One Hundred Years of Solicitude: Intellectual Property Law, 1900–2000*, 88 CAL. L. REV. 2187, 2228–31 (2000) (explaining how the Supreme Court’s mischaracterization of computer software as merely an algorithm led the Court to incorrectly ban patents on software for a time).

72. See, e.g., *id.* at 2190 (“Detailed, technology-specific provisions reflecting the passing concerns of a moment have proven difficult to adapt to new technologies.”). Of course, it may well be important to write rules with specific technologies in mind. Yet, excess specificity can have interesting consequences. For example, in conducting oversight, an office’s mission may be to assure compliance with legal requirements, and the office may therefore find it important to require a detailed description of the relevant technology being deployed and the agency’s implementing procedures governing its use. Indeed, the absence of such detail poses problems, since it may otherwise be difficult to ascertain compliance with general standards. However, creating detailed documentation for purposes of oversight risks technical translation errors, which could later result in compliance incidents if the implementation does not match the submitted documentation. Moreover, because technology changes rapidly and unpredictably, if an agency’s procedures are premised on a certain set of external technical conditions and those conditions unexpectedly change, program personnel will need to be alert to submit modifications.

73. See *supra* note 64 and accompanying text.

74. Reasoning by analogy is frequently encountered in judicial opinions. See generally Richard A. Posner, *Reasoning by Analogy*, 91 CORNELL L. REV. 761 (2006) (reviewing LLOYD L. WEINREB, *LEGAL REASON: THE USE OF ANALOGY IN LEGAL ARGUMENT* (2005)).

new situations must, of course, occur under the civil liberties protection infrastructure discussed earlier,⁷⁵ subject to congressional oversight and to judicial supervision where appropriate. Measures to review and enhance elements of this infrastructure, and to provide greater transparency, are in process.⁷⁶ Seen in this context, filling any policy gaps “the Brandeis way” appears to offer a helpful way forward, even in situations where comprehensive rule changes are ultimately deemed necessary.

V. Conclusion

Making technology choices at the intersections of privacy and security does not require tradeoffs. The IC need not stand paralyzed by the choice between its core mission to provide security and its solemn obligation to protect privacy and civil liberties. Instead, we should maintain the balance between security and liberty. We should ensure, on the one side, that a new technological capability is lawful, narrowly tailored to achieve an appropriate security purpose, and that there are no less intrusive means available, while we add, on the other side, counterbalancing privacy and civil liberties protections. We should look to Justice Brandeis’s example, which remains more relevant than ever: find core principles in our tried-and-tested rules, apply them to new changes in the technological landscape, and use those principles to help us clarify and, where necessary, update our rules and develop new protections. In the end, Yogi Berra’s⁷⁷ approach may prove truest of all: when facing a fork in the road between security and privacy, take it.

75. *See supra* note 31 and accompanying text.

76. *See, e.g.*, Exec. Order No. 13,526, 75 Fed. Reg. 707 (Jan. 5, 2010) (“Protecting information critical to our Nation’s security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.”).

77. *See supra* note 5 and accompanying text.

The Key Theory: Authenticating Decrypted Information in Litigation While Protecting Sensitive Sources and Methods

Nicholas J. Patterson*

Introduction

Since at least the beginning of the Cold War, the U.S. government has grappled with the difficulty of introducing deciphered encrypted information in litigation without exposing sensitive sources and methods. This Article describes a method for cutting that Gordian knot.¹

Encryption has been used since ancient times by militaries, spies, and others to communicate information covertly.² As encryption technology has evolved in complexity and decreased in expense with the advent of computer encryption, it has created new opportunities for foreign powers, foreign and corporate spies, terrorist groups, and criminals.³

* J.D., The University of Chicago Law School; M.Phil., Cambridge University; A.B., The University of Chicago. Counsel for National Security Law and Policy, National Security Division, United States Department of Justice. I greatly appreciate the help of the individuals listed below. I bear sole responsibility for any errors herein. For reading and commenting on drafts of this Article, I thank Matthew A. Anzaldi, Susan Kelley Koeppen, Alexander K. Haas, Philip Hamburger, Orin S. Kerr, Steven P. Lehotsky, Paul Ohm, Eric Posner, Dakota Rudesill, and Benjamin Wittes. For inviting me to the Texas Law Review Symposium and asking me to write this Article, I thank Robert Chesney and the Editorial Board of the Texas Law Review. For suggesting the subject of this Article, I thank Leonard Bailey. For providing assistance concerning the record in the *Wasp Network Case*, I thank Caroline Heck Miller. For providing advice and suggestions regarding Senator Daniel Patrick Moynihan's Commission on Protecting and Reducing Government Secrecy and the Venona project, I thank Mark A. Bradley. The views expressed in this Article are the author's alone and do not represent the position of the United States Department of Justice.

1. The term *Gordian knot* refers to "an intricate problem" and is derived from "a knot tied by Gordius, king of Phrygia, held to be capable of being untied only by the future ruler of Asia, and cut by Alexander the Great with his sword." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 540 (11th ed. 2003). Interestingly, the Gordian knot itself may have been a cipher. See ROBERT GRAVES, THE GREEK MYTHS § 83.4 (1960) (explaining that the knot may have symbolized the ineffable name of Dionysus which, enknotted like a cipher, would have been passed on through generations of priests and revealed only to the kings of Phrygia).

2. See Brendan M. Palfreyman, Note, *Lessons from the British and American Approaches to Compelled Decryption*, 75 BROOK. L. REV. 345, 349–50 (2009) (describing historical uses of cryptography and the development of cryptography over time).

3. See, e.g., *The Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 850 Before the H. Permanent Select Comm. on Intelligence*, 106th Cong. (1999) (statement of Janet Reno, Att'y Gen. of the United States), available at <http://www.justice.gov/archive/ag/testimony/1999/agintell071499.htm> ("[I]t will become far more difficult for the FBI, DEA, and other federal, state, and local, law enforcement agencies, faced with the rising threat from the criminal use of commercially available encryption, to protect the public from crimes such as terrorism, narcotics trafficking, economic fraud, and child pornography."); Palfreyman, *supra* note

This Article articulates a “Key Theory” method for introducing evidence derived from encrypted information while protecting the U.S. government’s sources and methods. Under the Key Theory, if the government were to introduce encrypted information with an unbroken chain of custody or as a record of a regularly conducted activity and provide a key or password in court that deciphers the information, the government would not have to explain how or where it obtained the key or password or how the key or password works. Rather, the government would only have to show that the key or password works to decrypt the information.

This Article articulates a theory to introduce evidence derived from encrypted information where the government has made the judgment to reveal that it can decrypt that information.⁴ Part I provides an overview of the history of encryption, explains the basics of how it works, and shows how it has both grown more difficult to decipher and easier for more people to encrypt with the advent of computer encryption. Part II discusses how protecting sources and methods has historically been a problem when introducing deciphered information as evidence in national security cases. As an example, this Article examines the Federal Bureau of Investigation’s (FBI) decision not to use the information deciphered from the Venona program’s Soviet wire transmissions in espionage prosecutions in the 1950s. Part III explains how evidence is authenticated in the U.S. legal system. Part IV details the legal reasoning behind the Key Theory and shows how a similar approach was applied in the *Wasp Network Case*.⁵ Part V considers arguments defendants may raise against the application of the Key Theory—including Sixth Amendment Confrontation Clause, *Brady*,⁶ and Jencks Act⁷ arguments—and explains why these arguments fail. Part VI describes how the Key Theory can also be used by litigants in civil litigation.

I. The History of Encryption and the Growth of Computer Encryption

Cryptography is “the enciphering and deciphering of messages in secret code or cipher.”⁸ To keep information secret, an individual will encrypt the information and make it unintelligible to unauthorized parties.⁹ An authorized party will decrypt or decipher an encrypted message to read the

2, at 350 (“Today, electronic encryption has become standard practice for governments, corporations, and, to a somewhat lesser extent, individuals.”).

4. As a threshold issue, the government has to make a determination whether it is willing to make public the fact that it has acquired and decrypted the information. There may be instances where the government determines that security considerations prevent it from revealing that it possesses the ability to acquire and decrypt and, therefore, that it will not use the Key Theory in litigation.

5. *United States v. Hernandez*, No. 98-0721-CR-JAL (S.D. Fla. 2001).

6. *Brady v. Maryland*, 373 U.S. 83 (1963).

7. 18 U.S.C. § 3500 (2006).

8. MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY, *supra* note 1, at 302.

9. Palfreyman, *supra* note 2, at 348.

hidden information.¹⁰ Encrypted text is referred to by cryptographers as “ciphertext,” and unencrypted or decrypted text is referred to as “plaintext.”¹¹

Governments, militaries, and individuals have used cryptography to safeguard information and communications throughout history.¹² The ancient Greeks used a primitive form of cryptography. Herodotus describes an individual having his shaved skull tattooed with a secret message and then, after his hair grew back, being sent to the recipient of the message, who had the messenger’s head shaved to reveal the message.¹³ In ancient Rome, Julius Caesar employed a more advanced method of cryptography—he employed the process of shifting every letter in the alphabet up three steps.¹⁴

Since ancient Greek and Roman times, encryption has evolved from simple to increasingly intricate ciphers—such as Napoleon Bonaparte’s Great Paris Cipher¹⁵—to complex mechanical devices—such as the Enigma machine used by Germany in World War II¹⁶ and one-time pads used by the Soviet Union¹⁷—to digital encryption of electronic data.

Currently, electronic encryption is regularly used by governments, corporations, and some individuals to protect information that is either in electronic storage or electronically transmitted.¹⁸ Due to the limits of current

10. *Id.* at 348–49.

11. Phillip R. Reiting, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 172 n.8.

12. Palfreyman, *supra* note 2, at 349.

13. 3 HERODOTUS, *THE HISTORY OF HERODOTUS* 198 (George Rawlinson trans., New York, D. Appleton & Co. 1866).

14. Adam C. Bonin, Comment, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495, 497 (1996).

15. Napoleon Bonaparte’s Great Paris Cipher contained approximately 1,400 coded elements. MARK URBAN, *THE MAN WHO BROKE NAPOLEON’S CODES* 127–28 (2001). Its deciphering by the British is alleged to have contributed to his defeat. *See id.* at 191–93 (noting the value of the information that deciphering the code gave to the British).

16. DAVID KAHN, *THE CODEBREAKERS: THE COMPREHENSIVE HISTORY OF SECRET COMMUNICATION FROM ANCIENT TIMES TO THE INTERNET* 421–23 (1996).

17. The Soviet Union used two layers of encipherment with telegrams: the Soviets would translate a plaintext message into code using a code book and then encrypt the message with random numbers taken from a set of “one-time pads,” the pads being “theoretically indecipherable as long as the pads were used only once.” Ellen Schrecker, *Stealing Secrets: Communism and Soviet Espionage in the 1940s*, 82 N.C. L. REV. 1841, 1846 (2004); *see also* JOHN EARL HAYNES & HARVEY KLEHR, *VENONA: DECODING SOVIET ESPIONAGE IN AMERICA* 25–28 (1999) (detailing the Soviet two-step enciphering process).

18. Palfreyman, *supra* note 2, at 350.

technology, encryption software programs¹⁹ can render data virtually indecipherable without access to the appropriate encryption key²⁰ or password.²¹

As Professor Orin S. Kerr has explained, because “encryption keys are in most cases impossible to guess—trying to guess a single key could occupy a supercomputer for millions of years—encryption offers Internet users” and users of computer encryption generally a degree of privacy in electronic “communications that remains unequalled in the physical world.”²² Unbreakable computer encryption has the potential to give spies, terrorists, hackers, child pornographers, and members of organized crime a powerful weapon to shield their communications from the U.S. government.²³

II. The Historical Problem of Introducing Decrypted Information as Evidence in National Security Prosecutions Without Exposing Sources and Methods

The U.S. government has wrestled with the issue of using deciphered information in national security cases without endangering sources and methods for decades. An example of the difficulty of using and authenticating national security information in prosecutions can be seen in the decision of the FBI not to use information from the Venona decryption program in espionage prosecutions. In February 1943, the U.S. Army’s Signal Intelligence Service, “the precursor to the National Security Agency, began a secret program . . . later codenamed VENONA,” whose initial mission “was to examine and exploit Soviet diplomatic communications[,] but after the program began, the message traffic included espionage efforts as well.”²⁴ The intercepted cables had been sent “between Moscow and the United States (mainly to and from contacts in New York and Washington).”²⁵ The cables

19. Some of these encryption programs, such as Pretty Good Privacy (PGP), are publicly available. See Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a “Reasonable Expectation of Privacy?”*, 33 CONN. L. REV. 503, 503 n.2 (2001) (explaining that PGP is a free software program that “uses public-key encryption to protect e-mail and data files”); PGP CORP., CORPORATE BACKGROUNDER 4 (2008), <http://download.pgp.com/pdfs/datasheets/PGP-Corporate-Backgrounder.pdf> (describing the background and history of PGP Corporation).

20. See Palfreyman, *supra* note 2, at 350 (explaining that an encryption key is “essentially a very long string of numbers whose length makes it extremely hard to memorize”).

21. See *id.* (explaining that a password activates an encryption key and is shorter and more easily remembered).

22. Kerr, *supra* note 19, at 503.

23. See *The Encryption Debate: Criminals, Terrorists, and the Security Needs of Business and Industry: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the S. Comm. on the Judiciary*, 105th Cong. 5 (1997) (statement of Sen. Patrick Leahy, Member, S. Comm. on the Judiciary) (acknowledging awareness of “‘bad’ uses of encryption by criminals” and spies).

24. National Security Agency, Venona (Jan. 15, 2009), http://www.nsa.gov/public_info/declass/venona/index.shtml. The first of six public releases of decrypted Venona messages was not made until 1995. *Id.* This release was followed by five more releases that made public all of the approximately 3,000 Venona translations. *Id.*

25. DANIEL PATRICK MOYNIHAN, *SECURITY: THE AMERICAN EXPERIENCE* 61 (1998).

were both coded and enciphered,²⁶ and “it remains a marvel” that approximately 2,900, a fraction of the thousands intercepted, “were ever broken.”²⁷

The information gained through this program “provided U.S. leadership with insight into Soviet intentions and treasonous activities of government employees” until the program ended in 1980.²⁸ The Venona decryptations showed the accuracy “of the information about Soviet espionage” that defecting Soviet agents “Whittaker Chambers (beginning in 1939) and Elizabeth Bentley (beginning in 1945) had provided to the American government.”²⁹ Ultimately, the Venona decryptations provided “some two hundred names or code names of Americans who were passing secret information to Soviet agents.”³⁰ The Venona files “are most famous for exposing Julius and Ethel Rosenberg . . . [and] the Soviets’ efforts to gain information on the U.S. Atomic bomb research and the Manhattan Project.”³¹ Additionally, the Commission on Protecting and Reducing Government Secrecy, chaired by Senator Daniel Patrick Moynihan, found that the Venona files settled the question of the complicity of Alger Hiss and Harry Dexter White.³²

This decrypted information created a dilemma for the U.S. government. The government had devastating evidence regarding Soviet spies that would facilitate—and in some cases make possible—their prosecution. However,

26. See *supra* note 17.

27. MOYNIHAN, *supra* note 25, at 61. Although the team began breaking some of the cables in the summer of 1946,

[t]he arduous decoding work began in 1943 and was done at Arlington Hall, a former girls’ school in Virginia; the setup resembled that of the Ultra project at Bletchley Park in wartime Britain, where German signals were intercepted and decoded. But unlike the British team, which had a smuggled copy of the encoding machine used by the Germans, the American team had only the coded cables themselves. Led by Meredith Knox Gardner, the code-breakers put in much hard work during World War II, but they broke nothing.

Id.; see also CHRISTOPHER ANDREW, FOR THE PRESIDENT’S EYES ONLY: SECRET INTELLIGENCE AND THE AMERICAN PRESIDENCY FROM WASHINGTON TO BUSH 178 (1995) (explaining how the volume of intelligence telegraphed to Moscow from the United States in the last year of World War II led to the reuse of one-time pads and made the cipher system vulnerable).

28. National Security Agency, *supra* note 24.

29. MOYNIHAN, *supra* note 25, at 61; see also HAYNES & KLEHR, *supra* note 17, at 93–115, 122–23, 150–51 (describing Elizabeth Bentley’s espionage activities for the Soviet Union and her defection); *id.* at 65–67, 125–26, 137–39, 227–28 (describing Whittaker Chambers’s espionage activities and his defection). For more in-depth, comprehensive treatments of Bentley and Chambers, see generally KATHRYN S. OLMSTED, RED SPY QUEEN: A BIOGRAPHY OF ELIZABETH BENTLEY (2002) and SAM TANENHAUS, WHITTAKER CHAMBERS (1997).

30. MOYNIHAN, *supra* note 25, at 62.

31. National Security Agency, *supra* note 24.

32. COMM’N ON PROTECTING AND REDUCING GOV’T SECRECY, REPORT OF THE COMMISSION ON PROTECTING AND REDUCING GOVERNMENT SECRECY, S. DOC. NO. 105-2 app. A, at A37 (1997) (“The complicity of Alger Hiss of the State Department seems settled. As does that of Harry Dexter White of the Treasury Department.”); see also MOYNIHAN, *supra* note 25, at 146 (explaining that “[w]ith the publication of the Venona documents, the evidence of Hiss’s guilt became public” and that “Hiss was indeed a Soviet agent and appears to have been regarded by Moscow as its most important”).

using the evidence in such prosecutions would risk exposing the sources and methods the government used to obtain the evidence.³³ In a 1956 memo, Assistant Director of the Domestic Intelligence Division of the FBI Alan H. Belmont counseled against introducing Venona information into evidence in the espionage prosecution of Judith Coplon—an analyst who had worked in the Foreign Agents Registration section of the U.S. Department of Justice, had access to FBI counterespionage files, and was arrested by the FBI in 1949 while handing over some of those files to a KGB officer.³⁴ He also advised against using Venona information in prosecutions of the Perlo group—which developed Soviet sources on the War Production Board, on a key Senate committee, and in the Treasury Department³⁵—and the Silvermaster group—which established contacts “not only in [the] Treasury and the Army Air Force but in the White House itself.”³⁶ Despite recognizing that the introduction of this evidence “could be the turning point” in such cases, and acknowledging that such information had been used in investigations that resulted in cases against a number of individuals, he concluded that attempting to use this information for prosecution “would not be in the best interests of the U.S. or the Bureau.”³⁷ Ultimately, the government was unsuccessful in its two attempts to prosecute Coplon³⁸ and did not prosecute the members of the Silvermaster³⁹ and Perlo groups.⁴⁰

A significant factor in the FBI’s decision was the potential disclosure of sources and methods that would have arisen from introducing the

33. Protecting sources and methods remains an issue. See 50 U.S.C. § 403-1(i)(1) (2006) (“The Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.”). The Key Theory described below presumes that the U.S. government is willing to disclose the fact that it can acquire and decrypt the information.

34. Memorandum from A.H. Belmont to L.V. Boardman (Feb. 1, 1956), in VENONA: FBI DOCUMENTS OF HISTORIC INTEREST 70–72, available at <http://foia.fbi.gov/venona/venona.pdf>; see also HAYNES & KLEHR, *supra* note 17, at 3, 158–60 (describing the intercepted communications concerning Coplon, her arrest, and the problems associated with the use of the communications in her prosecution).

35. See HAYNES & KLEHR, *supra* note 17, at 116–29 (describing the Perlo group’s members and their espionage activities).

36. *Id.* at 116.

37. Memorandum from A.H. Belmont to L.V. Boardman, *supra* note 34, at 61–62. Belmont described how such information had been used in investigations that led to the prosecution of, *inter alia*, Judith Coplon and Julius and Ethel Rosenberg, and how those “prosecutions were instituted without using [the] information in court.” *Id.* at 62. Additionally, the memorandum includes a handwritten note at the end of the summary of Belmont’s analysis that appears to be from FBI Director J. Edgar Hoover stating, “I agree.” *Id.*

38. See HAYNES & KLEHR, *supra* note 17, at 159–60 (describing how Coplon was tried and convicted twice, but each time an appellate court ordered a new trial after finding key evidence inadmissible due to lack of probable cause and attributing these findings to the government’s decision not to produce Venona decryptations and show that the decryptations were the basis of its actions).

39. See JOHN EARL HAYNES & HARVEY KLEHR, EARLY COLD WAR SPIES 32 (2006) (discussing the Silvermaster group and noting that “none of those . . . accused were ever convicted, or even indicted, for espionage”).

40. HAYNES & KLEHR, *supra* note 17, at 129.

information as evidence.⁴¹ Specifically, the FBI was concerned that defendants would request that privately hired cryptographers be allowed to examine the encrypted messages and the work of the government's cryptographers to exonerate their clients.⁴² Disclosure of this information and work, the FBI feared, would lead to the exposure of U.S. government techniques and practices in the field of cryptography to unauthorized persons and thus compromise the government's efforts in the communications intelligence field.⁴³ Also, this course could lead to the exposure of pending investigations.⁴⁴

III. The Requirement of Authentication

The Federal Rules of Evidence provide federal courts with wide latitude in authenticating evidence. Federal Rule of Evidence 901 sets forth the following general test: "The requirement of authentication . . . as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."⁴⁵ In other words, as long as there is sufficient evidence for a reasonable juror to find that the item is "genuine (or in the case of illustrative evidence, that it fairly and accurately depicts what it is claimed to illustrate), the authentication threshold is met."⁴⁶ The trial court does not need to determine that an item is

41. See Memorandum from A.H. Belmont to L.V. Boardman, *supra* note 34, at 70 (referencing the potential exposure of techniques and practices).

42. See *id.* (expressing concern that because the government would need its cryptographers to testify as experts for the information, the defense would request and would be permitted to have its own cryptographers examine not only information the government sought to introduce as evidence but all messages that were not decrypted).

43. *Id.*

44. Additionally, the FBI was concerned with, *inter alia*, the damage to the United States' efforts in the counterespionage field "if the Soviets learn[ed] of the degree of success" the United States had achieved in breaking the Soviets' codes—a consideration, as discussed above, that the government has to decide is outweighed by the need for prosecution before applying the Key Theory. *Id.* at 62. Unbeknownst to the U.S. government, the Soviets already knew that the United States had partially broken their codes "thanks to a spy among the code-breakers and thanks also to Soviet spy Kim Philby, British intelligence's liaison to the American intelligence services, whom the proud code-breakers had invited to tour Arlington Hall." MOYNIHAN, *supra* note 25, at 16. Some other concerns of Belmont's were as follows:

the question of law involved—whether or not the [redacted] information would be admitted into evidence as an exception to the hearsay evidence rule; . . . the fragmentary nature of the messages and the extensive use of cover names therein make positive identifications of the subjects difficult; . . . the political implications in this an election year; . . . the international repercussions and resultant Soviet propaganda when it is disclosed that the U.S. intercepted and worked on breaking Soviet coded messages when the countries were allied again[st] the Axis . . ."

Memorandum from A.H. Belmont to L.V. Boardman, *supra* note 34, at 61–62.

45. FED. R. EVID. 901(a).

46. Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 8 (2009).

authentic; rather it only needs to “determine that a reasonable juror could find that the item is authentic.”⁴⁷

Rule 901(b) provides nine examples of how materials can be authenticated.⁴⁸ The Rule specifically states that these examples are “[b]y way of illustration only, and not by way of limitation,”⁴⁹ and the Advisory Committee’s note expands on this idea stating that the examples are “meant to guide and suggest, leaving room for growth and development in this area of the law.”⁵⁰ Of these examples, the three most relevant to the instant analysis of the Key Theory are Rule 901(b)(1) (“Testimony of witness with knowledge. Testimony that a matter is what it is claimed to be.”),⁵¹ Rule 901(b)(4) (“Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances”),⁵² and Rule 901(b)(9) (“Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.”).

Additionally, the first two of these examples can be combined in the chain-of-custody doctrine to create “a hybrid form” of Rule 901(b)’s “listed methods.”⁵³ The chain-of-custody doctrine “involves both the testimony of one or more witnesses with knowledge [Rule 901(b)(1)] . . . and the distinctive characteristics of the evidence, taken in conjunction with circumstances [Rule 901(b)(4)].”⁵⁴ This doctrine applies to evidence that “is not readily identifiable and is susceptible to alteration by tampering, decay, or contamination.”⁵⁵ The litigant seeking to introduce such evidence must authenticate it by demonstrating “what the evidence was when gathered and that it has remained unchanged since then.”⁵⁶ The litigant must account for

47. *Id.*; see also *United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007) (recognizing the standard for authentication as “minimal”).

48. FED. R. EVID. 901(b)(1)–(9). Rule 901(b)(10) incorporates any other methods recognized by statute or court rule.

49. *Id.* R. 901(b).

50. *Id.* R. 901 advisory committee’s note.

51. Rule 901(b)(1) “contemplates a broad spectrum” of testimony, including testimony of a witness “accounting for custody through the period until trial, including laboratory analysis.” *Id.*

52. The Advisory Committee’s note on Rule 901 explains:

[C]haracteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety. Thus a document . . . may be shown to have emanated from a particular person by virtue of its disclosing knowledge of facts known peculiarly to him . . . ; similarly, a letter may be authenticated by content and circumstances indicating it was in reply to a duly authenticated one.

Id.

53. 5 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN’S FEDERAL EVIDENCE § 901.03[3] (Joseph M. McLaughlin ed., 2d ed. 2008).

54. *Id.*

55. *Id.*

56. *Id.*

the item from the time of seizure by law enforcement until presentation at trial.⁵⁷

Further, Federal Rule of Evidence 803(6)—under which records of regularly conducted activity are not excluded by the hearsay rule—can be used to bring into evidence information that is a record of regularly conducted business activity.⁵⁸ The element of unusual reliability of business records is said variously to be supplied by “systematic checking, by regularity and continuity which produce habits of precision, by actual experience of business in relying upon them, or by a duty to make an accurate record as part of a continuing job or occupation.”⁵⁹

The next Part discusses how the Key Theory works, both in theory and practice, and how the Rule 901(b) examples, the chain-of-custody doctrine, and the hearsay exception for records of regularly conducted activity can be used to authenticate plaintext derived from ciphertext under the Key Theory.

IV. The Key Theory: The Concept and How It Can Be Applied

Under the Key Theory, the government can authenticate decrypted information and have it admitted into evidence in court if it can demonstrate an unbroken chain of custody of the encrypted information or that the encrypted information is a record of a regularly conducted activity, and that a decryption key, password, or other means of decryption in its possession can decrypt the encrypted information. The government does not need to explain how the key, password, or other means of decryption was obtained or created.

The reasoning behind the Key Theory is that an encryption key or password, like a key to a locked door, simply makes accessible something already in existence; it does not alter the encrypted information or create something new. Decryption is a binary process: the key or password either deciphers or does not decipher the information. Further, just as it would not be necessary or efficient for a police officer to testify to issues regarding metallurgy or locksmithing as part of testifying that a key opens a locked door, a government witness demonstrating the Key Theory should not have to explain how the decryption process works. Therefore, for the purposes of authentication in litigation establishing admissibility, it should be sufficient to show that the encrypted information has remained unchanged since the government seized it or that it was a record of a regularly conducted activity and that the key or password deciphers the information.

57. *Id.*

58. FED. R. EVID. 803(6).

59. *Id.* R. 803(6) advisory committee’s note.

A. *The Method of Applying the Key Theory*

The method of applying the Key Theory is flexible and can be adapted to different circumstances. The basic elements of the Key Theory process are based on Federal Rules of Evidence 901 and 803(6)⁶⁰ and are: (1) showing either (a) that the government has maintained an unbroken chain of custody of the encrypted information, or (b) that the encrypted information is a record of a regularly conducted activity; and (2) providing a demonstration to the district court and jury of how the key or password decrypts a particular kind of encryption.

As an initial matter, to promote efficiency and relevance, the government should, in most cases where the Key Theory is applied, seek factual narrative testimony rather than expert testimony from its witnesses. That is, the prosecution can have a witness, who may or may not have expertise in the area as an incidental matter, testify in a factual manner—for instance, describing the process or steps he followed to decrypt the information—without the witness offering any opinions or even a non-opinion description of scientific processes. Having a witness present factual narrative testimony promotes a relevant and focused factual inquiry and efficient use of the time of the judge, jury, and litigants, which is encouraged by the Federal Rules of Evidence.⁶¹ The Key Theory is a simple process—a witness demonstrates that a key or password decrypts encrypted information—and does not require a witness to provide an opinion based on scientific, technical, or other specialized knowledge. Further, having a witness provide factual narrative testimony promotes trial efficiency. The government can use a single witness to show how encrypted information was seized and either that an unbroken chain of custody has been maintained or that the encrypted information was part of regular business records and then demonstrate the Key Theory. This provides a more streamlined process than having one witness testify to the former and a second testify to the latter. Calling a witness who only provides factual narrative testimony also promotes a more focused inquiry on cross-examination because such a witness, not held out as an expert, is not subject to the same kind of distracting and elaborate questioning about background and experience.⁶² Thus, employing witnesses to present the Key Theory who limit their testimony to factual narrative testimony helps pare back the case to its basic and essential elements and prevents detours into irrelevant and time-consuming areas of inquiry.⁶³

60. See *supra* Part III.

61. See, e.g., FED. R. EVID. 403 (excluding relevant evidence if its admission would be inefficient).

62. See *id.* R. 702 (requiring a witness who testifies as an expert to be “qualified as an expert by knowledge, skill, experience, training, or education”).

63. Choice of witnesses and limits on their examination can also be affected by motions in limine before the trial. See *id.* R. 103 (governing the procedure for admitting and excluding

1. *Chain of Custody.*—Demonstrating that the government has maintained an unbroken chain of custody generally lays a foundation for the introduction of the decrypted information into evidence. It also specifically sets the stage for the government's demonstration that the encryption key or password decrypts the information by showing that the government has in no way altered the information. It defuses any argument by opposing counsel that the key or password that the government presents in its demonstration is not a real key to the seized encrypted material but is instead a key to a version of the encrypted material altered by the government to implicate their client.

As mentioned above, the chain-of-custody doctrine is a hybrid of Federal Rule of Evidence 901(b)(1) ("Testimony of witness with knowledge. Testimony that a matter is what it is claimed to be.") and Rule 901(b)(4) ("Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.").⁶⁴ Prosecutors can use these two rules in the context of the Key Theory to have a government fact witness explain how the materials were seized, preserved, and not altered—in other words, that the encrypted materials being presented in court are the same as the encrypted materials originally seized—and to show how the materials are tied to the defendant.

Specifically, the government, when applying the Key Theory, could have a fact witness testify that the encrypted materials were obtained through a lawful search and seizure pursuant to a warrant. The witness can tie the encrypted materials to the defendant by explaining, for example, how the materials were seized from the defendant's residence or work place. The witness can then explain how he or she entered either the original version or an original unaltered copy—in the instance of a surreptitious search where it was necessary to make a copy rather than taking the original so that the defendants would not contemporaneously know the search occurred—of the encrypted information into evidence. In some instances, it may be possible for the witness to testify that he or she ensured the integrity of the original through a means such as write protecting a disk. The witness can then testify that he or she made true and accurate copies of this information to use as work copies. The government can use the work copies to examine and possibly decipher the encryption. The original or original unaltered copy will be entered into evidence. Upon the defendant's request, under the Federal Rules of Criminal Procedure, the government may be required to provide access to

evidence); GLEN WEISSENBERGER, WEISSENBERGER'S FEDERAL EVIDENCE § 1.03.4 (6th ed. 2009) ("[M]otions [in limine] may be made by either the party seeking admission or the party seeking exclusion, and are usually (although not always) made before trial.").

64. See *supra* notes 53–57 and accompanying text.

the original seized encrypted materials to the defense to inspect and copy; it also may choose to provide the defense a copy.⁶⁵

2. *Records of Regularly Conducted Activity.*—For certain types of evidence, such as acquisition of high-frequency radio transmissions, because the evidence was gathered as part of a regularly conducted activity, the record may be admissible pursuant to Federal Rule of Evidence 803(6).

3. *Demonstration.*—After the government has used the chain-of-custody doctrine to show that the encrypted materials have not been altered, the government can then demonstrate, pursuant to Federal Rule of Evidence 901(b)(9) (“Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.”), that the ciphertext corresponds to the proffered plaintext because the process of applying the key or password to the ciphertext results in the decryption of the information. The Advisory Committee’s note explains that Rule 901(b)(9) is “designed for situations in which the accuracy of a result is dependent upon a process or system which produces it,” and cites the examples of x-rays and computers.⁶⁶ The note also states that Example 9 “does not, of course, foreclose taking judicial notice of the accuracy of the process or system.”⁶⁷ This example can be used in the context of the Key Theory to show that in the process of decryption, when the key or password the government offers is used, it decrypts the encrypted information. The accuracy of the process or system can be seen in the fact that the key or password produces coherent plaintext rather than incoherent ciphertext.

The government should not have to demonstrate in court the decryption of all the files that are unlocked by the key and password to enter the files into evidence. It should be sufficient to have a government witness illustrate or describe the decryption on one document and then have the witness testify that the key or password similarly decrypted the other encrypted information the government seeks to introduce into evidence. The information can then be entered into evidence.

4. *Two Approaches to Applying the Key Theory.*—Depending on the circumstances of a case, the government may choose to take one of two approaches to implementing the Key Theory. First, the government, particularly in instances where there is a strong need to protect sensitive

65. See FED. R. CRIM. P. 16(a)(1)(E) (providing that “[u]pon a defendant’s request, the government must permit the defendant to inspect and to copy” tangible objects obtained from the defendant or that the government intends to offer in evidence).

66. FED. R. EVID. 901 advisory committee’s note.

67. *Id.* To the extent that a district court has questions about sources and methods and the way the decryption was accomplished, one way to address the court’s concerns might be through the use of procedures in the Classified Information Procedures Act, 18 U.S.C. app. 3 (2006).

sources and methods, can take a guarded approach. In this approach, the government only shows that the key or password decrypts the encrypted information and does not provide testimony regarding where or how the key or password was found or how it works. Second, the government may employ a rich-context method. Under this approach, in addition to showing that the key or password decrypts the encrypted information, the government can provide general information on where it found the key or password, explain generally how the key or password works, or both. The government would not have to explain: (1) how it knew where to find the key or password, (2) how it learned how the key or password works, or (3) the mechanics behind the key or password's operation.

B. *The Key Theory in Practice: The Wasp Network Case*

The *Wasp Network Case* provides helpful examples of how the government can apply a rich-context version of the Key Theory in litigation. However, although instructive, these examples should not obscure that a more austere, guarded Key Theory approach is also available.

1. *Background.*—On June 8, 2001, a federal jury in the U.S. District Court for the Southern District of Florida convicted five agents of the Directorate of Intelligence, Cuba's primary intelligence agency, of covert activity in the United States (including, as to three defendants, conspiracy to commit espionage)⁶⁸ concluding a multi-month trial that showed “a committed band of spies working to infiltrate South Florida's military installations and Cuban exile community.”⁶⁹ All five defendants were convicted of acting within the United States as agents of a foreign government without notification to the Attorney General, and also of conspiracy to do so and to defraud the United States concerning its governmental functions.⁷⁰ Three members of the group were convicted of conspiracy to commit espionage related to their efforts to penetrate military bases.⁷¹ One member of the group, Gerardo Hernandez, was found guilty of conspiracy to commit murder in connection with the deaths of four fliers from the “Brothers to the Rescue” Cuban-exile

68. See *United States v. Campa*, 529 F.3d 980, 991 (11th Cir. 2008) (detailing the convictions of Gerardo Hernandez, Rene Gonzalez, Antonio Guerrero, Ruben Campa, and Luis Medina), *cert. denied*, 129 S. Ct. 2790 (2009). The U.S. Court of Appeals for the Eleventh Circuit affirmed all convictions. *Id.* at 1018. While affirming all convictions, the Eleventh Circuit remanded the cases of three of the defendants for resentencing. *Id.* Resentencing occurred in October and December 2009; two of those defendants appealed, and the appeals are pending. Notice of Appeal, *United States v. Hernandez*, No. 98-0721-CR-JAL (S.D. Fla. Dec. 22, 2009).

69. Sue Anne Pressley, *Five Cuban Agents Guilty of Spying on U.S.*, WASH. POST, June 9, 2001, at A12.

70. Associated Press, *5 Cubans Convicted in Plot to Spy on U.S.*, N.Y. TIMES, June 9, 2001, at A12.

71. *Id.* Five other indicted members of the group pleaded guilty; some received reduced sentences in light of substantial assistance to the government. *Id.* Four indicted defendants were not arrested and are believed to be in Cuba. *Id.*

group—a “Miami-based organization that flew small aircraft over the Florida Straits in efforts to aid rafters fleeing Cuba”⁷²—who were shot down in 1996 in international airspace by Cuban MiGs.⁷³ The prosecution showed that Hernandez was instructed to steer fellow spies who had infiltrated Brothers to the Rescue away from targeted flights⁷⁴ and was instructed to deliver a message to Havana that led up to the shoot down.⁷⁵

In 1998, the agents were indicted as part of the 14-member, Florida-based spy group, who were known within the Directorate of Intelligence as *La Red Avispa*, or the Wasp Network.⁷⁶ The prosecution established that the defendants were referenced in their communications by code names, and that several were present in the United States under false identities, with false documentation and false life stories,⁷⁷ as the group followed through on assignments to penetrate Cuban-exile political groups and U.S. military installations—including Southern Command, which supervises U.S. military activities in the Caribbean and Latin America.⁷⁸

Prosecutors presented a case based largely on more than 1,200 pages of decrypted communications seized before or at the time of the defendants’ arrests in 1998.⁷⁹ A juror interviewed after the verdict said that the covert documents were the prosecution’s best evidence.⁸⁰ “It wasn’t the complete case, but it was damaging,” the juror said.⁸¹ “There wasn’t much the defense could say about them. They were found in their apartments, and they said a lot of damaging things.”⁸²

2. *Application of the Key Theory in the Wasp Network Case.*—In the *Wasp Network Case*, the prosecution could be characterized as having used what is described above as a rich-context version of the Key Theory method to authenticate decrypted information related to the Wasp Network and its activities. A close examination of how the prosecution authenticated

72. *Campa*, 529 F.3d at 988.

73. Pressley, *supra* note 69.

74. *Campa*, 529 F.3d at 988.

75. Pressley, *supra* note 69.

76. *Id.*

77. The difference between code names and false identities is that all defendants were referred to among themselves by code names, such as “Giro” and “Iselin,” but only some of the defendants, the careerist illegal intelligence officers, operated under false identities. See Brief for the United States at 10 n.9, *United States v. Campa*, 419 F.3d 1219 (11th Cir. 2005) (Nos. 01-17176, 03-11087) (“As part of the compartmentalization and secrecy that are hallmarks of intelligence networks . . . , defendants all had code names apart from false identities.”); *id.* at 4 (“[I]llegal intelligence officers . . . enter the U.S. illegally under false identities such as Hernandez, Medina and Campa . . .”).

78. Pressley, *supra* note 69.

79. Associated Press, *supra* note 70.

80. Gail Epstein Nieves, *Juror: Disk Made Spy Case Easy*, MIAMI HERALD, June 12, 2001, available at 2001 WLNR 3885684.

81. *Id.*

82. *Id.*

decrypted information from computer diskettes and high-frequency radio transmissions shows how the Key Theory can be applied in practice. The following subsections explain how the prosecution authenticated information that was decrypted using three decryption programs: Micro Star, The Typist, and Find.

a. Micro Star Decryption Program.—The prosecution first used what could be seen as a version of the Key Theory method during the direct examination of FBI Special Agent Vicente M. Rosado to introduce into evidence information on computer diskettes decrypted using the Micro Star program. Mr. Rosado was an FBI Special Agent assigned to the Computer Analysis Response Team—a group based in the FBI headquarters laboratory whose function is to “process and analyze computer evidence”—and he had a duty responsibility for “[f]oreign counter intelligence” related to Cuba.⁸³ He laid a foundation for the introduction of the evidence related to Micro Star by showing that he had participated in lawful searches and seizures (including surreptitious searches and seizures) based on warrants⁸⁴ and that the evidence had been held in an unbroken chain of custody and had not been altered.⁸⁵ He then demonstrated to the judge and jury how a password applied to a decryption method decrypted the information.⁸⁶

i. Chain of Custody.—In laying the foundation for admitting the evidence during direct examination by a federal prosecutor, Mr. Rosado first explained how the Government copied 981 disks during lawful searches of the residences of members of the Wasp Network.⁸⁷ Mr. Rosado explained that during the investigation of the Wasp Network his job was to use a machine to “copy computer evidence as found in the residence[s]” and “make sure no trace was left that [he] had been present [He] would just make [his] copies on site and leave everything as it was.”⁸⁸ Mr. Rosado also explained that the entries he made were pursuant to federal court orders for each time period at issue.⁸⁹ These searches and seizures culminated in a final overt search and seizure, pursuant to a search warrant, at the time that the defendants were arrested.⁹⁰

In addition to explaining the search and seizure process, Mr. Rosado explained the process he used to preserve the integrity of the diskettes he had

83. Transcript of Record at 1730, *United States v. Hernandez*, No. 98-0721-CR-JAL (S.D. Fla. 2001).

84. *Id.* at 1734–36.

85. *See id.* at 1745–48 (detailing for the court how he copied the disks, ensured they could not be overwritten, and placed them into evidence).

86. *Id.* at 1772–80.

87. *Id.* at 1898–99, 1902–03.

88. *Id.* at 1744.

89. *Id.* at 1736, 1748–52, 1754.

90. *Id.* at 1807.

made. To protect the diskettes he was downloading data onto and to prevent them from being altered or changed after he had copied data onto them, Mr. Rosado “moved a tab on the computer disk which write protects the diskette so no one else could write to it.”⁹¹ He then made copies of the diskettes he had made and “took the originals and placed them into our evidence.”⁹² These copies were “work copies” and were “true and accurate reproductions of the files that appeared on the disks” he had copied while searching the residences.⁹³

ii. Demonstration.—After laying this evidentiary foundation that, among other things, showed that the encrypted information had not been altered in any way, Mr. Rosado explained and demonstrated how a password used in conjunction with a decryption method decrypted information on the disks. At first, a large majority of the disks appeared to be “empty” or “appeared to have regular files.”⁹⁴ Mr. Rosado used a laptop computer to show what a computer diskette is, how it is read using a computer, and what a blank disk looks like.⁹⁵ He then inserted a copy of a diskette, which was entered into evidence as Exhibit D2, obtained during a search of the apartment of a member of the Wasp Network and showed that although it appeared blank when he checked the diskette’s directory and did a check-disk inquiry, he was eventually “able to find data on that disk.”⁹⁶ Mr. Rosado found that some of the program files⁹⁷ found on other disks “acted on the apparent blank disk in order to decrypt or bring forth data.”⁹⁸ These files did not declare themselves to be decryption or “breakout” programs and were not labeled as such; rather they appeared to be everyday commercial programs.⁹⁹

The prosecutor then asked Mr. Rosado to place another copy of a disk made during a search of a defendant’s apartment, labeled Exhibit D3 and subsequently entered into evidence, into his laptop.¹⁰⁰ Mr. Rosado opened what appeared to be a word processing program on the disk called Micro Star, and he confirmed that there were no files on the disk other than a file explaining how to use Micro Star.¹⁰¹ He then testified that if one used the word processor’s open command on such a disk, ordinarily one would not

91. *Id.* at 1747.

92. *Id.* at 1748.

93. *Id.*

94. *Id.* at 1764.

95. *Id.* at 1759, 1763.

96. *Id.* at 1765–66.

97. A program file is “[a]n electronic file containing commands and instructions for execution by a computer.” WEBSTER’S NEW WORLD TELECOM DICTIONARY 392 (2008).

98. Transcript of Record, *supra* note 83, at 1767.

99. *Id.*

100. *Id.* at 1768.

101. *Id.* at 1770–71.

expect entering a name would access a file.¹⁰² He then showed that when he went to the “open” command and typed the password *afinacion* or entered that file name, the program asked him to “insert a diskette.”¹⁰³ Mr. Rosado testified that ordinarily when one tries to open a specific word processing file, one would expect the program would either show the text of the file or say that no text exists.¹⁰⁴ After this explanation, Mr. Rosado inserted Exhibit D2, the diskette that had previously seemed to be blank, and three different documents in Spanish, which would print out to several pages of text, appeared on the computer screen.¹⁰⁵ Mr. Rosado testified that he had previously reviewed the Spanish-language text, and it was a report that referenced, among other things, Brothers to the Rescue activities; it was from “Iselin,” a code name for defendant Rene Gonzalez, to “Giro,” a code name for defendant Gerardo Hernandez;¹⁰⁶ and it appeared to be an account of meetings and results of meetings.¹⁰⁷ He explained that the text included two additional reports.¹⁰⁸

The prosecutor then further examined Mr. Rosado, laying a foundation for these files and numerous other decrypted files to be entered into evidence. The prosecutor presented three notebooks containing government files depicting Mr. Rosado’s “work product” in printed-out form.¹⁰⁹ Mr. Rosado explained that when he went through this disk and others like it, he saved the decrypted information to another disk or printed it out in decrypted form.¹¹⁰ He testified that those pages “truly and accurately reproduce[d] the files” as he “broke them out from other disks” and that he worked with, broke out, and produced the text for all of the exhibits in the books.¹¹¹ He also testified that he used different decryption files found in programs in addition to the Micro Star program to decrypt some of these disks.¹¹² Following this testimony, the district court admitted into evidence the Government exhibits of the decrypted plaintext Spanish-language files in the three notebooks.¹¹³ Later, English translations were admitted into evidence.¹¹⁴

Mr. Rosado also explained where he obtained the password or key to the Micro Star decryption files and generally how he used the password or

102. *Id.* at 1771–72.

103. *Id.* at 1772.

104. *Id.*

105. *Id.* at 1773.

106. *See* United States v. Campa, 529 F.3d 980, 980 (11th Cir. 2008) (stating in the case caption that Rene Gonzalez was also known as Iselin and that Gerardo Hernandez was also known as Giro).

107. Transcript of Record, *supra* note 83, at 1774.

108. *Id.*

109. *Id.* at 1785.

110. *Id.* at 1774–75.

111. *Id.* at 1785–86.

112. *Id.* at 1786.

113. *Id.*

114. *Id.* at 2672.

key with the decryption files. He stated that the word *afinacion* is “a password or key to allow” the Micro Star word processing program “to operate in a manner other than its intended” word processing purpose.¹¹⁵ This password or key is necessary to start the decryption process.¹¹⁶ He also testified and demonstrated to the court on his laptop that this key or password *afinacion* can be found on the same disk as the Micro Star decryption program by using Norton Utilities Disk Editor, a widely available commercial program, to access the sector of the disk that contains the key or password.¹¹⁷ He noted that the word *afinacion* stands out from the other types of characters because it “is a word that doesn’t really fit into what I would expect to find on a disk that has a program.”¹¹⁸

Thus the prosecution can be seen to have used a rich-context version of the Key Theory method with Mr. Rosado to enter into evidence the decrypted information from the specific demonstration file and other files decrypted with the Micro Star decryption program and the password or key *afinacion*. This allowed the prosecution to enter this information into evidence based on data within the parameters of the disks. Although Mr. Rosado provided background on how the government obtained and used the key or password *afinacion* and the Micro Star decryption program, he did not purport to explain or analyze theoretical or scientific concepts of decryption.

b. The Typist Decryption Files.—The prosecution used similar approaches, which could also be seen as applications of the Key Theory, during the direct examinations of Myron Broadwell and Kenneth W. Hart to introduce information from high-frequency radio transmission¹¹⁹ intercepts that had been decrypted with The Typist decryption files found on diskettes from the defendants’ residences. Mr. Broadwell laid the foundation for the admission of records of the encrypted transmissions by explaining how the transmissions were collected and transcribed as a regular professional practice of the FBI, and Mr. Hart demonstrated how The Typist, when used with keys and passwords, decrypted the intercepts.

i. Records of Regularly Conducted Activity.—On direct examination, Mr. Broadwell—a supervisory special agent with the FBI’s investigative-technologies branch of the laboratory division and the supervisor of the Data Collection Facility, whose staff listens to high-frequency broadcasts using shortwave radio receivers¹²⁰—explained the process by which the FBI collected and made a record of the radio transmissions.

115. *Id.* at 1778–79.

116. *Id.* at 1779.

117. *Id.* at 1779–81.

118. *Id.* at 1783–84.

119. *See id.* at 2447 (explaining that high-frequency radio transmissions are “radio transmissions that exist in the frequency bandwidth from approximately 3 to 30 megahertz”).

120. *Id.* at 2444, 2446.

Mr. Broadwell explained that his staff listened to recordings of these radio broadcasts, “transcribe[d] what is generally Morse code being transmitted,” and archived the transcriptions.¹²¹ Mr. Broadwell testified that with the Morse code broadcasts instead “of a voice it would be a series of tones, short and long in the Morse code coding scheme.”¹²² Although these broadcasts are readily audible to anyone who has a commercially available shortwave radio, because the broadcasts are in Morse code, they are not readily comprehensible.¹²³ His staff transcribed the Morse code, which is transmitted in five character groups, into alpha characters—rather than numbers—and typed that into a word processing program for generating a transcript.¹²⁴ He explained that such transcription is a regularly conducted duty or practice of the FBI.¹²⁵

Mr. Broadwell testified that he had been asked to collect or retrieve certain archived transcripts and to place them on storage or transfer media, and then identified a color photocopy of a computer disk that had been received in evidence as one onto which he “copied certain selected transcriptions of high frequency broadcasts”; he also identified a notebook as containing printed-out versions of the retrieved Morse code transcripts.¹²⁶ Additionally, he explained that the transcription appeared as “a series of random letters,” which would not make sense to a person.¹²⁷ The prosecution then moved for admission of the notebook pages reflecting the encrypted text of the messages, and the district court admitted it over the objections of the defense.¹²⁸

The prosecution subsequently moved to admit into evidence similar pages of the notebook reflecting older transcripts through a combination of Federal Rule of Evidence 803(6) and the chain-of-custody doctrine.¹²⁹ Mr. Broadwell testified that during the time the transcriptions were made, such transcriptions were the professionally, regularly conducted activity of the FBI, and that once the transcriptions were made, they were put into “files and placed into safes” and remained within the custody of the data-collection facility.¹³⁰

ii. Demonstration.—With the encrypted information admitted into evidence on this foundation, the prosecution called Mr. Hart to “testify

121. *Id.* at 2447–48.

122. *Id.* at 2448.

123. *Id.*

124. *Id.* at 2449.

125. *Id.* at 2452.

126. *Id.* at 2452–54.

127. *Id.* at 2453.

128. *Id.* at 2457–59.

129. *Id.* at 2488.

130. *Id.*

to the breaking out of these messages into plain text.”¹³¹ Mr. Hart—a computer specialist,¹³² forensic examiner¹³³ for the FBI laboratory division, and member of the Computer Analysis Response Team—testified that he used decryption files that Mr. Rosado had acquired from the defendants’ residences to decrypt the encrypted high-frequency radio messages provided by Mr. Broadwell.¹³⁴

Similarly to Mr. Rosado, Mr. Hart performed a computer demonstration to show how materials seized from the defendants’ residences could be used to decrypt information. Mr. Hart explained that one of the seized disks contained a “program called The Typist, which appeared to be a game” or “tutorial involving typing skills.”¹³⁵

To begin the demonstration, Mr. Hart inserted the disk into the computer—with screens in the courtroom showing the judge, the jury, and the defense the computer screen—and showed the directory of files that appeared on the disk, including The Typist file.¹³⁶ He explained that The Typist file stood out on the disk because it is a boot disk¹³⁷ and “the first four files are DOS operating system files and Typist is on there all alone.”¹³⁸ Mr. Hart then opened The Typist file¹³⁹ and showed how the regular game works.¹⁴⁰

Although The Typist initially appeared to be a regular game, Mr. Hart explained that if he typed the password or key *GIRASOL*, the program stopped acting as a typing-proficiency game and threw up a prompt for a file name.¹⁴¹ This did not appear to be part of the regular game, and the program appeared to have been altered.¹⁴²

Mr. Hart then opened The Typist program, started the game, entered the password *GIRASOL*, and when prompted entered the file name for an encrypted file.¹⁴³ Text then appeared on the screen in the courtroom in Spanish.¹⁴⁴ Mr. Hart explained that he used The Typist program against

131. *Id.* at 2459.

132. *See id.* at 2572 (describing a computer specialist as a “person who extracts, examines and/or produces data from digital related evidence”).

133. *See id.* at 2571 (describing forensic examiners as individuals who “examine and extract and present digital evidence from computers, computer type evidence and storage media”).

134. *Id.* at 2584.

135. *Id.* at 2590–91.

136. *Id.* at 2594.

137. A boot disk is a disk that allows a computer to start. Tech Terms Computer Dictionary, <http://www.techterms.com/definition/bootdisk>. The most common type is an internal hard drive. *Id.*

138. Transcript of Record, *supra* note 83, at 2595.

139. *Id.* at 2595–96.

140. *Id.* at 2596–97.

141. *Id.* at 2599.

142. *Id.*

143. *Id.* at 2605–06.

144. *Id.* at 2606–07.

other texts that appeared in the Government's book of exhibits and was able to obtain plaintext for other messages.¹⁴⁵ He also testified that there were other versions of The Typist program on other disks that were capable of decrypting certain messages that The Typist program he used for his courtroom demonstration could not decrypt.¹⁴⁶ Mr. Hart then testified that the text on the screen was the same as on a page in the Government's exhibit notebook, and the court admitted the page into evidence over the defense's objections.¹⁴⁷

Mr. Hart testified that he applied The Typist program and obtained plaintext for each of the exhibits reflected on a chart that detailed, among other things, the separate exhibits and the means the Government used to decrypt them.¹⁴⁸ Each of the relevant exhibits in the exhibit book had a first page of ciphertext (which was in evidence through Mr. Broadwell's testimony) and a second page of plaintext in Spanish, which Mr. Hart had decrypted using the program disks as enumerated on the chart.¹⁴⁹ The prosecution then moved into evidence approximately thirty-seven decrypted plaintext Spanish exhibits related to The Typist program over the objections of the defense.¹⁵⁰

Mr. Hart also explained the process pointing to the password or key, *GIRASOL*. He testified that the word "was embedded inside the program file itself" and that he found it "mostly by visual inspection."¹⁵¹ He then demonstrated that he could use the program Norton Disk Editor—a utility program that can be used to view low-level data for programs, drives, and files—to view the contents of the executable file The Typist.¹⁵² When he applied Norton Disk Editor, it showed a hexadecimal¹⁵³—a base-16 numbering system—and ASCII—American Standard Code for Information Interchange,

145. See *id.* at 2607 (referencing a chart introduced by the prosecution reflecting that certain messages were capable of being decrypted and producing plaintext using The Typist).

146. *Id.* at 2608.

147. *Id.* at 2610–11.

148. *Id.* at 2616.

149. *Id.*

150. *Id.* at 2616–17. As with the decrypted diskettes, in plaintext Spanish, introduced during Mr. Rosado's testimony, a translator's subsequent testimony later provided the foundation for introduction of the English translations of the decrypted messages introduced through Mr. Hart's testimony, comprising the third page of each tabbed entry in the notebook. See *id.* at 2669 (describing the translated diskette decrypts being entered into evidence); *id.* at 2826 (describing the translated high-frequency radio transmission decrypts being entered into evidence).

151. *Id.* at 2611.

152. *Id.* at 2612.

153. The hexadecimal system is "a different method of representing numbers than the base-10 system [used] in every day practice." Tech Terms Computer Dictionary, <http://www.techterms.com/definition/hexadecimal>. In the hexadecimal system, "each digit can have sixteen values instead of ten." *Id.* For example, "[t]he values of a hexadecimal digit can be: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F." *Id.* Although "computers process numbers using the base-2, or binary system, it is often more efficient to visually represent the numbers in hexadecimal format" because "it only takes one hexadecimal digit to represent four binary digits." *Id.*

the standard character set used by computers and made up of letters, numbers, and symbols—equivalent of the file.¹⁵⁴ He then looked through the ASCII display of the contents of the file, which was quite lengthy, “looking for groups of letters, five to seven characters in length.”¹⁵⁵ In a particular area of the column, he found the letters *HKUEXUS*, which he explained were a cipher for the password or key *GIRASOL*: “Basically you take your first letter and you go backwards one step in the alphabet and you will get the letter G by going back one character” and for the second letter “[y]ou go back two steps in the alphabet and it progresses on through until eventually you wind up with *GIRASOL*.”¹⁵⁶

In this way, the Key Theory can be seen to account for how the prosecution authenticated information derived from The Typist decryption program. The prosecution laid the foundation for entering the information into evidence by having Mr. Broadwell explain how the encrypted information was obtained and Mr. Rosado testify how the decryption programs were seized and preserved. The prosecution built on this foundation by having Mr. Hart testify and demonstrate how the password or key, combined with The Typist program, decrypted the information.

As with Mr. Rosado’s testimony, the prosecution had Mr. Hart explain and demonstrate generally how The Typist program worked and where the password or key was found, but did not present an analytic or theoretical explanation of the decryption or other scientific processes underlying it.

c. Find Decryption Program.—The prosecution also can be seen to have applied the Key Theory in entering information decrypted with the Find decryption program into evidence. Mr. Hart testified that although the last two exhibits in the notebook of exhibits, which were also taken from high-frequency radio transmissions, were not capable of being broken out with The Typist program, another decryption program called Find.EXE on one of the seized disks was able to decrypt the files.¹⁵⁷ He also testified that two of the seized disks contained the decryption key, and another disk had the password, *safelight*.¹⁵⁸ Additionally, Mr. Hart explained that, similar to what he had demonstrated with The Typist program, the password *safelight* was embedded in hexadecimal material.¹⁵⁹

Rather than asking Mr. Hart to perform a computer demonstration of the Find decryption program as he had done with The Typist program, the prosecution had Mr. Hart testify to the process whereby he decrypted the two

154. Transcript of Record, *supra* note 83, at 2612–13.

155. *Id.* at 2613–14.

156. *Id.* at 2614.

157. *Id.* at 2622–23.

158. *Id.* at 2624.

159. *Id.*

files The Typist had been unable to decrypt.¹⁶⁰ He stated that he would start the “Find program much like [he] started the Typist one,” only he “put the password right on the command line of the program. It would be find space then the password used.”¹⁶¹ Instead of getting the find options from using the program, he would then be presented with an options menu screen, in which case he “could receive messages, send messages or exit the program.”¹⁶² At that point, to receive the decryption process, he would use the option to receive the messages; then he would type the name of the file to be decrypted, and the Find program would give the user options for which hard drive to use with the decryption key disk.¹⁶³ Once the user put the decryption key disk in the appropriate hard drive and hit enter, Mr. Hart explained, “if it is the correct disk for that message or program, it will show up on the screen similar to Typist, the translated or decrypted text of your original message.”¹⁶⁴ He then testified that he was able to decrypt the two files described above with this process and that the plaintext in the Government’s exhibit book was the same as the decrypted text he had produced.¹⁶⁵ The district court then admitted the plaintext of these two files in the exhibit book into evidence.¹⁶⁶

Again, the prosecution was able, through what could be characterized as an application of the Key Theory, to move decrypted information into evidence within the parameters of the seized material. The prosecution had the witness generally show what the password was, how the password and decryption keys were discovered, how the decryption program worked, and that it worked on the two files.

Thus, the *Wasp Network Case* provides examples of how the government can carefully authenticate decrypted information according to the principles of the Key Theory by laying a solid evidentiary foundation through the chain-of-custody doctrine or the business-records exception to the hearsay rule and then demonstrating how the key or password decrypts the encrypted information.

V. Defense Arguments Against the Key Theory and Why They Fail

Defense counsel may raise a number of arguments against the Key Theory. The following are the most likely to be raised. For the reasons set forth below, each of these objections is flawed. The common flawed thread in each objection is a lack of acknowledgement of the simple, binary nature of the Key Theory.

160. *Id.*

161. *Id.*

162. *Id.*

163. *Id.* at 2625.

164. *Id.*

165. *Id.* at 2625–26.

166. *Id.* at 2626.

A. Sixth Amendment Confrontation Clause Objection

Under the Sixth Amendment's Confrontation Clause, "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him."¹⁶⁷ In *Crawford v. Washington*,¹⁶⁸ the Supreme Court increased the scope of the Confrontation Clause in trials.¹⁶⁹ Justice Scalia's opinion made any "testimonial" out-of-court statement inadmissible if the accused did not have the opportunity to cross-examine the witness and the witness is unavailable at trial.¹⁷⁰ The Court refused to determine whether laboratory test results are testimonial evidence subject to the Confrontation Clause.¹⁷¹ In *Melendez-Diaz v. Massachusetts*,¹⁷² the Court held that certificates of analysis (which state the results of state laboratory tests) are testimonial evidence that may not be admitted without accompanying live testimony by the analyst who conducted the tests.¹⁷³ Defendants can cross-examine the affiants under their Sixth Amendment right of confrontation.¹⁷⁴

There is little national security case law following these decisions so far. However, it would appear that *Melendez-Diaz* would not apply to the Key Theory process because the government conducts a demonstration in front of the defendant, the judge, and the jury. Further, the witness who performs the demonstration can be cross-examined by the defense. Pursuant to the Federal Rules of Evidence, such cross-examination should be limited to the factual demonstration itself.¹⁷⁵ It should not be necessary to have the demonstrating witness explain scientific concepts related to decryption. A police officer does not have to testify how a key works in a lock or where he found

167. U.S. CONST. amend. VI.

168. 541 U.S. 36 (2004).

169. *See id.* at 60, 68 (condemning the Court's prior Confrontation Clause test as at once overly broad and too narrow, "often fail[ing] to protect against paradigmatic confrontation violations" and devising a new test in which all evidence that could be considered testimonial would be subject to scrutiny under the Sixth Amendment).

170. *Id.* at 68. Testimonial means any statements that an objectively reasonable person in the declarant's situation would have deemed likely to be used in court. *See Davis v. Washington*, 547 U.S. 813, 822 (2006) (holding that statements made in a police interrogation are testimonial when the circumstances objectively indicate that there is not an ongoing emergency and the primary purpose of the interrogation is to discover facts for possible use in a prosecution).

171. *The Supreme Court, 2008 Term—Leading Cases*, 123 HARV. L. REV. 153, 202 (2009); *see also Crawford*, 541 U.S. at 68 ("We leave for another day any effort to spell out a comprehensive definition of 'testimonial.' Whatever else the term covers, it applies at a minimum to prior testimony at a preliminary hearing . . . and to police interrogations.").

172. 129 S. Ct. 2527 (2009).

173. *Id.* at 2542; *see also* Posting of Lyle Denniston to SCOTUSblog, <http://www.scotusblog.com/?s=law+need+not+bow+to+chemistry> (June 25, 2009, 15:36 EST) (summarizing the *Melendez-Diaz* decision).

174. *See Melendez-Diaz*, 129 S. Ct. at 2532 (holding that the defendant was entitled to be confronted with the affiants at trial).

175. *See* FED. R. EVID. 611(b) ("Cross-examination should be limited to the subject matter of the direct examination . . .").

the key to show how he opened a door,¹⁷⁶ and a government witness in an encryption case should not have to testify how a key or password was obtained or works with an encryption program to demonstrate how the key or password decrypts the information.

B. *Brady and Jencks Act Objections*

Defendants could also argue that the Key Theory violates the Supreme Court's *Brady v. Maryland*¹⁷⁷ decision and the Jencks Act.¹⁷⁸ However, because of the binary nature of the Key Theory, *Brady* and Jencks Act obligations should not apply to the demonstration, and the government should follow its *Brady* and Jencks Act obligations regarding the decryption process.

In *Brady*, the Supreme Court ruled that suppression by the prosecution of evidence favorable to a defendant who has requested it violates due process.¹⁷⁹ The prosecutor must disclose evidence or information that would prove the innocence of the defendant or mitigate the defendant's sentence.¹⁸⁰ For example, prosecutors must disclose exculpatory evidence known only to the police.¹⁸¹ The prosecutor has a duty to review the police's investigatory files and disclose anything that tends to prove the innocence of the defendant.¹⁸²

The Jencks Act governs production of statements and reports of prosecution witnesses during federal criminal trials.¹⁸³ The Act provides the following:

In any criminal prosecution brought by the United States, no statement or report in the possession of the United States which was made by a Government witness or prospective Government witness (other than the defendant) shall be the subject of subpoena, discovery, or inspection *until* said witness has testified on direct examination in the trial of the case.¹⁸⁴

Brady and the Jencks Act are not obstacles to the Key Theory. The Key Theory involves a simple mechanical function—a key or password unlocking encrypted information—so *Brady* and the Jencks Act would not apply because the process would not be germane to exculpatory information. The key or password would either work or would not work. If the key or password

176. See *id.* R. 201(b) (describing judicial notice as appropriate when the fact is “generally known within the territorial jurisdiction of the trial court”); *id.* R. 402 (“Evidence which is not relevant is not admissible.”).

177. 373 U.S. 83 (1963).

178. 18 U.S.C. § 3500 (2006).

179. 373 U.S. at 86.

180. *Id.* at 87.

181. *Kyles v. Whitney*, 514 U.S. 419, 438–39 (1995).

182. *Id.*

183. 18 U.S.C. § 3500.

184. *Id.* § 3500(a).

works, there would be no exculpatory information. If the key or password does not work, the materials in question would not be authenticated, and *Brady* and the Jencks Act would not be necessary.

The government should follow its *Brady* and Jencks Act obligations regarding the decryption process.

C. *Reciprocity and Multiple Keys*

The defense may request to have its experts examine the encrypted information and the password or key. One result of the government allowing the defense to examine the encrypted information is that the defense may produce another key or password that deciphers the ciphertext into different, less incriminating plaintext than that offered by the government. The government can respond to this argument in two ways. First, the government can state that most computer encryption, due to its complexity, will only have one key or password and hide only one plaintext message and that the message that the government has decrypted is the true message. Second, the government can explain that it is possible for an encrypter to combine two encrypted pieces of information into a single file so that a second key will open a second, innocent message and that this disinformation is just another form of encryption. The government can seek to show how this second encryption has been used to hide the incriminating encryption.

The government and the defendant can then ask the trial court, pursuant to Federal Rule of Evidence 104(a) (“Preliminary questions concerning . . . the admissibility of evidence shall be determined by the court . . .”), to authenticate their respective decrypted information and let the fact finder decide which information it should give weight to, considering the totality of the circumstances. To make this request, the defense would have to show that there is a basis for the defense’s version of the decryption. The defense could not just produce a purported plaintext and demand that it be admitted without laying a foundation showing that it was, in fact, decrypted from the ciphertext with an actual key or password. In this way, the government’s sensitive sources and methods would be protected and the relevant information would be authenticated.

D. *Defendant Claims Not to Have Been in Possession of Key, Decryption Method, or Encrypted Materials*

The defendant may also argue that the plaintext derived from an encrypted file should not be admitted into evidence because either the defendant had the encrypted file but not a key, password, or other decryption method, or the defendant had the decryption method, but the defendant claims it was not in possession of the encrypted information. This objection does not stand because under Federal Rules of Evidence 901 (“Requirement of Authentication or Identification”) and 402 (“Relevant Evidence Generally Admissible; Irrelevant Evidence Inadmissible”), it is only necessary to

produce evidence sufficient to support a finding that the item is what its proponent claims it to be and that it is relevant to the case. Thus, under the Key Theory, it is enough to show that the encrypted information in the possession of the defendant can be opened by a key or password, or that the key or password in possession of the defendant opens the encrypted information and that the encrypted information is relevant to the case in order to authenticate the resulting plaintext and have it admitted into evidence.¹⁸⁵ As long as the trial court authenticates the information and allows it into evidence, the court or jury can decide how much weight to give it.¹⁸⁶

VI. The Key Theory's Applicability to Civil Litigation

Although this Article has focused on the government's ability to use the Key Theory in prosecutions, the legal concepts of the Key Theory are also applicable to admission of evidence in civil cases. Civil litigants could potentially use the Key Theory to protect sources and methods related to national security and trade secrets.¹⁸⁷ However, strategically the court's indulgence of national security concerns might not be as great in a civil matter. Additionally, the pretrial deposition process of civil litigation might make it harder to control questioning regarding sources and methods underlying the decryption process.

185. The defendant might argue that if the information cannot be linked somehow to the defendant, it might lack sufficient relevance to be admitted into evidence. This objection lacks merit because under Federal Rules of Evidence 901 ("Requirement of Authentication or Identification") and 402 ("Relevant Evidence Generally Admissible; Irrelevant Evidence Inadmissible"), it is only necessary to produce evidence sufficient to support a finding that the item is what its proponent claims it to be and that it is relevant to the case. While defense objections of lack of nexus to the defendant could go to relevance, it is doubtful that a proponent would offer such evidence where there is no provable nexus to the defendant, at least circumstantially; the weight and significance of the nexus would be a jury question.

186. See FED. R. EVID. 104(a) ("Preliminary questions concerning . . . the admissibility of evidence shall be determined by the court . . ."); *id.* R. 104(e) ("[Rule 104] does not limit the right of a party to introduce before the jury evidence relevant to weight or credibility."). Once the evidence has been admitted, the government's concern for protecting cryptographic sources and methods continues. Although preliminary questions of admissibility are for the court, not the jury, and may be heard by the court outside of the jury's presence, *id.* R. 104(a), (c), the defense retains the right to cross-examine, before the jury, as to matters going to weight or credibility, *id.* R. 104(e). The reach of such cross-examination into cryptographic sources and methods may stress the Key Theory approach of limiting such inquiry. The government should be prepared to make careful argument and presentation to the trial court, perhaps with an advance motion in limine, concerning distinctions between cross-examination on sources and methods that may be said fairly to go to issues of weight and credibility, versus using cross-examination to probe government sources and methods just for free discovery or information gathering as to it.

187. See FED. R. CIV. P. 26(c)(1)(G) (allowing for protective orders requiring "that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way"); *Autotech Tech. Ltd. P'ship v. Automationdirect.com, Inc.*, 237 F.R.D. 405, 414 (N.D. Ill. 2006) (entering an attorneys'-eyes-only protective order to protect confidential trade secret information).

Conclusion

In these ways, the Key Theory offers a process for the government to authenticate decrypted information without exposing sensitive sources and methods. The Key Theory can be used both to protect national security and promote a more efficient litigation process.

Mending Walls: Information Sharing After the USA PATRIOT Act

Nathan Alexander Sales*

*Something there is that doesn't love a wall,
That sends the frozen-ground-swell under it,
And spills the upper boulders in the sun;
And makes gaps even two can pass abreast.*
—Robert Frost, “Mending Wall”

Introduction.....	1795
I. Two Cheers for Information Sharing	1799
II. Walls: Past and Present	1806
A. The Life and Times of the FISA Wall	1808
B. National Security Act of 1947	1813
C. Posse Comitatus Act	1819
D. Privacy Act	1830
III. Recalibrating the Law and Policy of Information Sharing.....	1836
A. Pretext Concerns	1837
B. Firewall Concerns	1841
C. Republicanism Concerns	1844
D. Privacy Concerns	1847
Conclusion	1853

Introduction

The conventional wisdom is that the USA PATRIOT Act tore down the wall.¹ The conventional wisdom is mistaken.

It was the summer of 2001, and FBI agents were frantically trying to locate a suspected al Qaeda operative named Khalid al-Mihdhar. Toward the end of August, Steve Bongardt, who was working the criminal investigation

* Assistant Professor of Law, George Mason University School of Law. I'm grateful to Bill Banks, Nate Cash, Bobby Chesney, Craig Lerner, Greg McNeal, Hugo Teufel, and Todd Zywicki for helpful comments on earlier versions of this Article. Special thanks to the Center for Infrastructure Protection and Homeland Security for generous financial support. I worked on a number of information-sharing initiatives while serving at the U.S. Departments of Justice and Homeland Security, but the opinions expressed in this Article are solely mine.

1. See, e.g., RICHARD A. POSNER, PREVENTING SURPRISE ATTACKS 122 (2005) (arguing that the PATRIOT Act “accomplished” the goal of “eliminating artificial barriers to the pooling of intelligence data”); Fred F. Manget, *Intelligence and the Criminal Law System*, 17 STAN. L. & POL’Y REV. 415, 420 (2006) (“The wall is gone.”).

of the USS *Cole* bombing, received an e-mail from one of the Bureau's intelligence officials; it mentioned that al-Mihdhar might have entered the United States. His curiosity piqued, Bongardt picked up the phone and asked his colleague to tell him more. What he got was an order to delete the message; it was sent to him by accident. Bongardt then fired off an angry e-mail: "Whatever has happened to this—someday somebody will die—and wall or not—the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.'"²

He was right. A few weeks later Khalid al-Mihdhar helped hijack American Airlines Flight 77 and crash it into the Pentagon.

After 9/11, it was widely agreed that national security officials needed to do a better job sharing information with one another.³ The free flow of data, it was argued, would help them "connect[] the dots" and prevent future attacks.⁴ An early example of this consensus was the USA PATRIOT Act,⁵ which amended a provision in the Foreign Intelligence Surveillance Act (FISA) that prevented intelligence officials at the FBI from exchanging data with criminal investigators.⁶ Yet even in PATRIOT's wake, a number of walls remain on the statute books.⁷ These legal constraints have attracted virtually no attention, either in academic circles or elsewhere. "[A]ny suggestion that there is still a 'wall' is not considered politically correct."⁸ The issue may have escaped notice, but that does not make it unimportant. The remaining restrictions on information sharing have the potential to affect the full range of agencies with national security responsibilities, from the Intelligence Community to the Armed Forces to law enforcement. They also potentially cover the entire spectrum of data that could be relevant to

2. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 271 (2004) [hereinafter 9/11 COMMISSION REPORT]; LAWRENCE WRIGHT, THE LOOMING TOWER: AL-QAEDA AND THE ROAD TO 9/11, at 353–54 (2006).

3. See 9/11 COMMISSION REPORT, *supra* note 2, at 416–19 (discussing the need for improved information sharing in the Intelligence Community); POSNER, *supra* note 1, at 26, 28 (urging improved cooperation between private and public agencies); Michael V. Hayden, *Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 247, 257–60 (2005) (calling for expanded information sharing); David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487, 518, 521–22 (2006) (analyzing the benefits of abolishing the FISA wall); Craig S. Lerner, *The USA PATRIOT Act: Promoting the Cooperation of Foreign Intelligence Gathering and Law Enforcement*, 11 GEO. MASON L. REV. 493, 524–26 (2003) (discussing some benefits of information sharing); Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 951–59 (2006) (discussing which information should be shared and when).

4. 9/11 COMMISSION REPORT, *supra* note 2, at 416.

5. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered titles of U.S.C.).

6. See *id.* § 218 (codified at 50 U.S.C. § 1804(a)(6)(B) (2006)) (permitting the use of FISA when a "significant purpose of the surveillance is to obtain foreign intelligence information").

7. See *infra* Part II.

8. Grant T. Harris, Note, *The CIA Mandate and the War on Terror*, 23 YALE L. & POL'Y REV. 529, 554 (2005).

counterterrorism operations, from electronic-surveillance intercepts to satellite imagery to industrial-facility vulnerability assessments.

This Article attempts to fill that gap in the literature. It has three goals: to weigh the advantages and disadvantages of information sharing; to identify some of the remaining legal restrictions on data exchange, as well as their policy justifications; and to consider whether these laws' underlying values can coexist with expanded sharing.

Part I discusses some of the benefits and costs of data exchange. A principal advantage of sharing is that it enables intelligence agencies to better detect national security threats. By assembling individual tiles that by themselves reveal little, information sharing allows analysts to see the entire mosaic of enemy intentions. Sharing also allows agencies to specialize in the collection of various different types of information; these market niches produce efficiency gains that result in better intelligence product. Yet sharing has its downsides. Data exchange can compromise sensitive intelligence sources and methods by increasing the likelihood that they will leak. It can flood intelligence analysts with troves of data, making it harder to distinguish signal from noise and reinforcing preconceptions about hostile powers' capabilities and intentions. And sharing can burden the privacy interests of persons to whom the data pertains.

Part II analyzes statutory restrictions on information sharing and their policy justifications. It begins with the prototypical wall—FISA's "primary purpose" requirement, which crippled information sharing from the mid-1990s up to the 9/11 attacks. The wall sought to prevent "pretext." It was feared that law enforcement officials might ask intelligence officials to collect evidence for use in criminal proceedings; FISA kept cops from evading the legal limits on domestic surveillance by commissioning spies to do the dirty work for them.

I then turn to some of the remaining statutory restrictions on information sharing. The National Security Act of 1947 bars the CIA from exercising "police, subpoena, or law enforcement powers" or engaging in "internal security functions."⁹ Similar to the FISA wall, the 1947 Act thus prevents spies from engaging in pretextual surveillance at the behest of cops. It also reflects "firewall" concerns—the notion that, while it might be appropriate to use unsavory intelligence techniques in the foreign sphere, the government should not operate the same way domestically. The Act's strictures could prevent the CIA from swapping information with federal law enforcement officials, most notably the FBI. A second restriction is found in the Posse Comitatus Act,¹⁰ which makes it a crime to "use[] any part of the Army or the Air Force as a posse comitatus or otherwise to execute the

9. 50 U.S.C. § 403-4a(d)(1) (2006).

10. 18 U.S.C. § 1385 (2006).

laws.”¹¹ Posse Comitatus is another firewall statute; it insulates domestic law enforcement from the more violent practices that characterize military operations. The Act also reflects “republicanism” concerns—the idea that the Armed Forces must always be subordinate to civilian authorities. The sweeping Posse Comitatus rule may prevent the Armed Forces from sharing information with domestic authorities in the aftermath of a terrorist attack or natural disaster by, for example, providing the FBI with intelligence about the attack site or offering tactical advice on how to manage the disaster zone. The Privacy Act of 1974 offers a third example. It promotes “individual privacy” in two senses: freedom from government observation and the ability to control how information about oneself is presented to the outside world. A restrictive reading of the Act—in particular, the requirement that routine disclosures of covered records must be “compatible with the purpose for which [they were] collected”¹²—could prevent, for example, U.S. Customs and Border Protection (Customs) from sharing data about arriving container ships with National Security Agency (NSA) officials who want to exploit it to screen for terrorist stowaways. In short, the 1947 Act, Posse Comitatus, and the Privacy Act are overbroad. Congress had good reasons to enact these statutes, but they sweep so broadly that they imperil desirable information sharing that does not threaten the harms about which Congress justifiably was concerned.

Part III considers whether it is possible to promote data exchange while remaining faithful to these laws’ underlying pretext, firewall, republicanism, and privacy concerns. The answer, I argue, is yes. My analysis is informed by rational-choice theories of bureaucratic action and focuses on individual and institutional incentives within military and intelligence agencies. It is unlikely that information sharing between the FBI and the CIA under the 1947 Act will raise meaningful pretext problems. The CIA will have strong incentives to decline requests by its bureaucratic rival to collect evidence for use in criminal proceedings because doing so would harm the CIA’s own interests. Similarly, sharing probably won’t raise firewall concerns. Data exchange can actually promote firewall principles by mitigating agencies’ incentives to mount aggressive operations in inappropriate spheres. Republicanism concerns do not justify sharing restrictions; the potential harms are both slight and unlikely to materialize. And information sharing can preserve privacy values even more effectively than a strict prohibition on data exchange by reducing agencies’ incentives to engage in privacy-eroding surveillance.

A few preliminary observations are needed. First, this Article suffers from the same shortcomings that plague virtually all efforts to write about highly classified national security matters—a dearth of publicly available

11. *Id.*

12. 5 U.S.C. § 552a(a)(7) (2006).

information. A good deal of data about how these statutory barriers affect information sharing among military, intelligence, and law enforcement players presumably remains hidden from public view. In its absence, the most we can hope to do is offer conjectures or educated guesses. Second, eliminating the statutory barriers discussed in this Article will not, without more, lead to the free flow of information. Agencies aren't exactly clamoring to share with one another; as I've argued elsewhere, officials have strong incentives to hoard data, and information sharing will be stymied unless these incentives are recalibrated.¹³ Still, modifying legal rules to permit more sharing is an important first step. Statutory restrictions on data exchange reinforce agencies' worst instincts, ensuring that even less information changes hands.

I. Two Cheers for Information Sharing

The post-9/11 consensus is that information sharing is a good thing. There is "near universal agreement" that "fighting terror will require deeper coordination than existed heretofore between law enforcement agencies, the CIA, and the military."¹⁴ Data exchange is worthwhile because it enables officials to piece together the intelligence mosaic, an especially important task in conflicts with nontraditional adversaries such as terrorist organizations.¹⁵ Also, sharing produces efficiency gains by allowing different intelligence agencies to specialize in collecting particular kinds of information.¹⁶ So why only two cheers? Because sometimes data exchange can harm the government's national security interests, to say nothing of the privacy interests of the people to whom the information pertains.

The principal advantage of information sharing is that it enables intelligence analysts to better detect threats against the United States. Taken individually, a piece of information might not reveal anything about an adversary's intentions or capabilities.¹⁷ But seemingly innocuous data can become more meaningful, and more sinister, when aggregated with other information.¹⁸ This is known as the mosaic theory.¹⁹ "[I]ntelligence gathering is 'akin to the construction of a mosaic'; to appreciate the full import of a single piece may require the agency to take a broad view of the

13. See Nathan Alexander Sales, *Share and Share Alike: Intelligence Agencies and Information Sharing*, 78 GEO. WASH. L. REV. 279, 303–13 (2010) (arguing that intelligence agencies hoard to protect their influence and autonomy).

14. Noah Feldman, *Choices of Law, Choices of War*, 25 HARV. J.L. & PUB. POL'Y 457, 482 (2002); see also *supra* note 3.

15. See David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628, 630–31, 645–46, 651 (2005) (discussing the mosaic theory and its increased prominence after 9/11).

16. Hayden, *supra* note 3, at 258.

17. Pozen, *supra* note 15, at 630.

18. *Id.*

19. *Id.*

whole work.”²⁰ One tile may not suggest much at all, but the larger mosaic might. The mosaic theory traditionally has been offered as a reason why the government might resist the release of a particular piece of information, as in response to a FOIA request.²¹ Yet it is as much a theory of intelligence analysis as it is a theory of nondisclosure. As long ago as the Revolutionary War, General George Washington—“America’s first spymaster”²²—recognized the importance of collecting and aggregating apparently unrelated pieces of information. “Every minutiae should have a place in our collection, for things of a seemingly trifling [sic] nature when conjoined with others of a more serious cast may lead to very valuable conclusions.”²³

A related benefit is that information sharing can reduce the likelihood of catastrophic intelligence failures.²⁴ “[T]he intelligence failures that hurt the worst have not been those of collection but rather those of dissemination.”²⁵ Some scholars believe that breakdowns in information sharing contributed to our failure to anticipate the attack on Pearl Harbor.²⁶ In the months before December 1941, American cryptologists had broken the principal code for Japan’s diplomatic communications and intercepted a number of increasingly alarming messages that Japan regarded conflict with the United States as inevitable.²⁷ Intelligence officers also determined that Japan had changed its naval call signs on November 1 and again on December 1, moves that were regarded “as signs of major preparations for some sort of Japanese

20. *J. Roderick MacArthur Found. v. FBI*, 102 F.3d 600, 604 (D.C. Cir. 1996) (citation omitted) (quoting *In re United States*, 872 F.2d 472, 475 (D.C. Cir. 1989)); see also *United States v. Marchetti*, 466 F.2d 1309, 1318 (4th Cir. 1972) (explaining that “[t]he significance of one item of information may frequently depend upon knowledge of many other items of information”).

21. See, e.g., *CIA v. Sims*, 471 U.S. 159, 178 (1985) (upholding the CIA’s refusal to divulge identities of private researchers participating in the Agency’s MKULTRA program, because “bits and pieces of data ‘may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself’” (quoting *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980))).

22. NATHAN MILLER, *SPYING FOR AMERICA* 5 (1989).

23. Letter from George Washington to Lord Stirling (Oct. 6, 1778), in 13 *THE WRITINGS OF GEORGE WASHINGTON FROM THE ORIGINAL MANUSCRIPT SOURCES, 1745–99*, at 39 (John C. Fitzpatrick ed., 1936); see also Hayden, *supra* note 3, at 258 (discussing the importance of sharing information that appears to be of little or no intelligence value).

24. Many factors besides sharing breakdowns contribute to faulty intelligence, including analysts’ cognitive biases, the “crying-wolf effect” of past false alarms, and so on. See POSNER, *supra* note 1, at 85–86; RICHARD A. POSNER, *UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM* 22–29 (2006). Even if data had flowed freely in the months before the 9/11 attacks, it’s far from clear that officials would have overcome these other obstacles to make the right intelligence calls. See MARK M. LOWENTHAL, *INTELLIGENCE: FROM SECRETS TO POLICY* 256–57 (4th ed. 2009). Enhanced information sharing may help stave off intelligence failure, but it doesn’t guarantee success.

25. Stewart A. Baker, *Should Spies Be Cops?*, *FOREIGN POL’Y*, Winter 1994–1995, at 36, 43.

26. ROBERTA WOHLSTETTER, *PEARL HARBOR: WARNING AND DECISION* 277–78 (1962).

27. *Id.* at 382, 385–86.

offensive.”²⁸ Yet these clues about Japan’s possible intentions were never pooled and integrated:

[N]o single person or agency ever had at any given moment all the signals existing in this vast information network. The signals lay scattered in a number of different agencies; some were decoded, some were not; some traveled through rapid channels of communication, some were blocked by technical or procedural delays; some never reached a center of decision.²⁹

Information sharing is also advantageous because it allows intelligence agencies to specialize in collecting different kinds of data, thereby producing efficiency gains. Consider the alternative: a system in which agencies only gain access to information they’ve collected on their own. Such an “eat what you kill” regime would result in wasteful redundancies, as agencies duplicated each others’ collection capabilities. Resources that the FBI might use more productively to intercept electronic communications within the United States would be diverted to replicating NSA overseas signals-intelligence assets. Those inefficiencies mean less intelligence would be produced. (This is not a mere hypothetical. When NSA officials in 2001 refused to hand over intercepts of Osama Bin Laden’s satellite telephone calls, the FBI made plans to conduct electronic surveillance by building its own antennae in Palau and Diego Garcia.³⁰) By contrast, an intelligence system based on information sharing allows agencies to carve out their own market niches. Agencies can focus their collection efforts on areas where they enjoy a comparative advantage—for example, the FBI’s comparative advantage in gathering information relating to domestic crimes, the CIA’s comparative advantage in gathering data from overseas spies, and so on. Sharing ensures that agencies will not be disadvantaged by specializing; they will still, through a system of trade, have access to data collected by others. The result is to lower the system’s overall costs of producing intelligence assessments.

Sharing also has the potential to encourage “competitive analysis,”³¹ which can result in better advice to policy makers. In particular, sharing increases the number of agencies capable of engaging in what’s known as

28. *Id.* at 385.

29. *Id.* But see David Kahn, *The Intelligence Failure of Pearl Harbor*, FOREIGN AFF., Winter 1991, at 138, 148 (“The intelligence failure at Pearl Harbor was not one of analysis, as Wohlstetter implies, but of collection.”).

30. WRIGHT, *supra* note 2, at 344.

31. See LOWENTHAL, *supra* note 24, at 14 (explaining that “competitive analysis” is “based on the belief that by having analysts in several agencies with different backgrounds and perspectives work on the same issue, parochial views more likely will be countered—if not weeded out—and proximate reality is more likely to be achieved”). Intelligence agencies “compete” in the sense that they vie with one another to produce the analytical outputs—threat assessments, reports, etc.—on which senior decision makers rely. In other words, agencies compete for more influence over policy makers, more prestige among their peers, and, to a lesser extent, enhanced budgets. See Sales, *supra* note 13, at 305.

“all source intelligence.” All source means that an agency’s analytical products incorporate data from many different collection sources, not just the ones over which that particular agency has control.³² Three such entities currently exist (the CIA, the Defense Intelligence Agency, and the State Department’s Bureau of Intelligence and Research³³); information sharing can lead to the emergence of others. Sharing enables analysts to examine the widest possible range of information, including data gathered by other agencies. The result is a system of competitive analysis in which multiple agencies consult a common pool of information to tackle the same intelligence questions. The previous paragraph argued that redundant intelligence collection is inefficient, but not all redundancy is wasteful;³⁴ cars come with seat belts and air bags, and drivers are safer for having them both. Redundant collection seems the very essence of waste; little is gained when five different agencies intercept the same e-mail.³⁵ But redundant intelligence analysis can be beneficial. Competitive analysis helps ensure that policy makers are exposed to diverse perspectives; it also helps counteract groupthink tendencies.³⁶

Information sharing may produce even greater benefits in conflicts with terrorists than in traditional warfare between nation-states.³⁷ Indications that a conventional attack is imminent are comparatively easy to detect; it isn’t hard to figure out what the Soviets have in mind when they mobilize 20,000 tanks to the border of West Germany.³⁸ But asymmetric warfare often involves precursor acts that by themselves appear innocent.³⁹ The warning signs of a terrorist attack could be as innocuous as a Nigerian named Umar Farouk Abdulmutallab boarding a Detroit-bound flight in Amsterdam on Christmas Day.⁴⁰ Their sinister implications can only be discerned when

32. See LOWENTHAL, *supra* note 24, at 72.

33. *Id.* at 38.

34. See Anne Joseph O’Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CAL. L. REV. 1655, 1675–84 (2006) (discussing some costs and benefits of redundancy among intelligence agencies).

35. See *id.* at 1679–80 (arguing that redundant information collection can increase costs without providing proportional benefits).

36. See LOWENTHAL, *supra* note 24, at 14, 139; William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1151, 1193 (2003); O’Connell, *supra* note 35, at 1676, 1689, 1731–32. Competitive analysis also has its downsides. “The existence of an alternative analysis, especially on controversial issues, can lead policy makers to shop for the intelligence they want or cherry-pick analysis, which also results in politicization.” LOWENTHAL, *supra* note 24, at 135.

37. See Swire, *supra* note 3, at 955–57 (discussing the changed landscape of warfare and its effect on intelligence).

38. See *id.* at 957 (“One important feature of the Cold War was that enemy mobilization was often graduated and visible.”).

39. See LOWENTHAL, *supra* note 24, at 133.

40. See Mark Hosenball et al., *The Radicalization of Umar Farouk Abdulmutallab*, NEWSWEEK, Jan. 11, 2010, at 37 (discussing Abdulmutallab’s personal background and the steps he took in his failed bombing attempt); Eric Lipton et al., *Review of Jet Bomb Plot Shows More Missed Clues*,

integrated with other pieces of information—for example, intercepts suggesting that al Qaeda intended to use a Nigerian to attack the United States around the holidays, intercepted e-mail traffic between Abdulmutallab and an anti-American cleric in Yemen, and warnings from Abdulmutallab's father that his son had become radicalized.⁴¹ Information sharing enables intelligence analysts to cross-check seemingly innocent facts against other signs of possible danger, thereby approaching the comparative certainty of conventional threat assessments.⁴²

Widespread data exchange has its benefits, but it also can harm the government's national security interests in several ways. Sharing increases the likelihood that sensitive intelligence will be compromised, whether through espionage (acquisition by a foreign power) or through leaks (disclosures to unauthorized persons, such as the news media).⁴³ The more people who are privy to a secret, the greater the danger it will be exposed. "Bulkheads in a ship slow movement between the ship's compartments, just as restrictions on sharing classified information slow the communication traffic between intelligence services. But in both cases there is a compelling safety rationale."⁴⁴

Still, the risk that sharing might compromise sensitive data seems exaggerated. Cold War Era information-access standards such as compartmentalization rules and "need to know" requirements were designed to counter a particular type of threat: espionage by a traditional nation-state adversary such as the Soviet Union.⁴⁵ They may be less vital in today's asymmetric conflicts with international terrorists.⁴⁶ Sharing restrictions still play an important role in preventing espionage by rival nations, such as Iran or North Korea.⁴⁷ But terrorist groups like al Qaeda have not proven as adept at placing spies in the American Intelligence Community.⁴⁸ At least as to

N.Y. TIMES, Jan. 17, 2010, at A1 (detailing intelligence failures in connection with the 2009 Christmas Day terrorist plot).

41. Hosenball et al., *supra* note 41, at 37.

42. See Hayden, *supra* note 3, at 258 (arguing that pooling "the data points of human intelligence, imagery, or law enforcement" could result in "information of high value to national security").

43. See POSNER, *supra* note 1, at 102–04 (recounting concerns about sharing information).

44. *Id.* at 103.

45. See Mark A. Chinen, *Secrecy and Democratic Decisions*, 27 QUINNIPIAC L. REV. 1, 28–29 (2009) (claiming that compartmentalization and similar policies were adopted in response to the Cold War).

46. See *id.* (suggesting that Cold War Era information-access policies are not as effective in conflicts with terrorists).

47. See David Morgan, *U.S. Adopts Preemptive Counterintelligence Strategy*, WASH. POST, Mar. 6, 2005, at A7 (reporting on new counterintelligence measures that were implemented to frustrate espionage efforts by China, Russia, Iran, North Korea, Cuba, and Libya).

48. See POSNER, *supra* note 24, at 215 (stating that terrorist organizations have less sophisticated intelligence operations than foreign states). *But see* Richard A. Oppel, Jr. et al., *Suicide Bomber in Afghanistan Was a Double Agent*, N.Y. TIMES, Jan. 5, 2010, at A1 (reporting that

information related to terrorist threats, then, the risks of espionage seem weaker. Of course, the danger that classified terrorism-related information might leak remains significant. Witness, for example, newspaper stories about the NSA's warrantless Terrorist Surveillance Program, secret CIA prisons in Central Europe, and so on.⁴⁹ But it might be possible to mitigate the risks of espionage and leaks with countermeasures other than sharing restrictions, such as electronic audit trails that record which officials have accessed a particular piece of information.⁵⁰

Sharing also can harm national security by producing a "flooding effect"—by inundating analysts with massive amounts of information.⁵¹ Roberta Wohlstetter argues that intelligence analysis is akin to trying to locate a faint "signal" hidden amid a mass of "noise."⁵² Information sharing can increase the amount of noise, making the signals even harder to detect. Sharing thus can overwhelm analysts, preventing them from detecting threats they otherwise would have found if only they hadn't been swamped with data.⁵³ Even worse, the flooding effect can lead to analytical distortions. By deluging analysts with unmanageable troves of data, sharing can reinforce their preconceptions about hostile powers' capabilities and intentions and blind them to unexpected threats.⁵⁴ In other words, sharing can exacerbate confirmation bias.⁵⁵ Analysts might cope with the reams of new information by fixating on the data points that confirm their preexisting biases and ignoring the ones that do not.⁵⁶ The result is analytical ossification, as established theories are reinforced and alternatives go unnoticed.⁵⁷

Concerns about flooding are legitimate, but they don't justify wholesale limits on information sharing. It is true that analysts' cognitive limitations are an imperfect way to filter data. But so are sharing restrictions. In a system that uses sharing limits as a filter, what determines whether data from one agency reaches another is not an informed, disinterested judgment about

an al Qaeda suicide bomber who killed seven CIA officers at a CIA base in Afghanistan was a double agent).

49. See, e.g., Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, WASH. POST, Nov. 2, 2005, at A1 (revealing the CIA's covert prison system for some al Qaeda captives); James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1 (reporting the existence of an NSA program to eavesdrop on certain international communications without court orders).

50. See MARKLE FOUND., *MOBILIZING INFORMATION TO PREVENT TERRORISM: ACCELERATING DEVELOPMENT OF A TRUSTED INFORMATION SHARING ENVIRONMENT* 7–8 (2006) (touting the benefits of certain defenses against leaks, such as electronic audit trails).

51. POSNER, *supra* note 1, at 104.

52. WOHLSTETTER, *supra* note 26, at 387, 393.

53. See *id.* at 387 (explaining that data overload can cause intelligence officers to sift through "all sorts of information that is useless and irrelevant").

54. See POSNER, *supra* note 1, at 116–17 (arguing that analysts respond to voluminous data by using their preconceptions to filter it).

55. *Id.* at 121.

56. *Id.*

57. *Id.*

whether or not it would be useful.⁵⁸ The decisive factor is likely to be a rival agency's self-serving determination about whether the exchange would benefit its interests or harm them.⁵⁹ Sharing restrictions are an exceedingly coarse way to separate signal from noise. A better way to prevent analysts from being inundated with data might be to rely on automated filtering technologies. The CIA reportedly is developing image-recognition technology that enables computers to match photographs with exemplars stored in a database.⁶⁰ The Office of the Director of National Intelligence also is said to be experimenting with an automated system that can scan databases of foreign surveillance videos and identify suspicious behavior.⁶¹ And computers are often tasked with running keyword queries ("al Qaeda," "jihad," and the like) against intercepted phone calls and e-mails.⁶² Human beings would only need to inspect what passed the automated filters. (Still, this seems an imperfect solution to the flooding effect. "Even in the age of computers, few technical shortcuts have been found to help analysts deal with the problem.")⁶³

It's not just the government that stands to lose from data exchange; sharing also can harm the privacy interests of the persons to whom the data relates.⁶⁴ Specifically, information sharing interferes with one's interest in preventing the government from observing personal facts.⁶⁵ The sharing of previously collected data amounts to fresh observation in several senses. First, sharing increases the number of officials with access to an otherwise private fact; the more officials who observe it, the greater the privacy harms.⁶⁶ Second, and more importantly, information sharing enables the government to integrate isolated units of data and thereby discover new information about the person:

[W]hen combined together, bits and pieces of data begin to form a portrait of a person. The whole becomes greater than the parts. This occurs because combining information creates synergies. When analyzed, aggregated information can reveal new facts about a person

58. See *supra* note 13 and accompanying text.

59. See *id.*

60. See LOWENTHAL, *supra* note 24, at 73.

61. Walter Pincus, *Finding a Way to Review Surveillance Tape in Bulk*, WASH. POST, Mar. 10, 2009, at A11.

62. See, e.g., Michael Hirsh, *The NSA's Overt Problem*, WASH. POST, Jan. 1, 2006, at B1 (bemoaning the NSA's "primitive" technique of running random keyword searches for Islamist taglines).

63. LOWENTHAL, *supra* note 24, at 117.

64. *But cf.* Kris, *supra* note 3, at 520 (arguing that sharing restrictions "do[] not provide much protection for privacy").

65. See, e.g., Julie E. Cohen, *Examined Lives, Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1371, 1375 (2000) ("'[P]rivacy' might encompass an enforceable right to prevent the sharing of . . . personally-identified data . . .").

66. *Cf.* *Whalen v. Roe*, 429 U.S. 589, 602-03 (1977) (recognizing that the right to information privacy is threatened by increased exposure of that information).

that she did not expect would be known about her when the original, isolated data was collected.⁶⁷

This is the same insight that informs the mosaic theory: integration creates new information.⁶⁸ Just as data aggregation can reveal new insights into al Qaeda's capabilities or plans, it can also reveal new insights into a person's private thoughts and actions.

Besides harming one's privacy interest in avoiding unwanted observation, information sharing also can undermine one's privacy interest in controlling data about oneself. Sharing interferes with the ability of data subjects to manage the dissemination of personal information and, ultimately, how they choose to present themselves to the outside world:

What advocates regard as being fundamentally at stake in the claim to informational privacy is *control* of personal information. . . . [T]o speak of a right of informational privacy is to invoke a "claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others."⁶⁹

The problem here is not so much that information sharing prevents data subjects from keeping personal information confidential; the problem is that sharing has the potential to undermine data subjects' autonomy.⁷⁰ Still, while it's certainly the case that information sharing can undermine privacy, sharing actually has the potential to promote privacy interests. This is so because, as I argue below, in some circumstances sharing can be a substitute for fresh privacy-eroding surveillance.⁷¹

II. Walls: Past and Present

The USA PATRIOT Act may have brought down one wall, but others remain on the statute books. This section begins with a brief discussion of the FISA wall and its underlying policy concerns. It then surveys several

67. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 507 (2006); cf. Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 139 (2008) (arguing that data retention and aggregation practices "threaten to convert many of the government surveillance activities now subject to a warrant requirement into the sort of 'indirect' surveillance at issue in—and unprotected by—[*United States v. Miller*], 425 U.S. 435 (1976)]").

68. See *supra* text accompanying notes 17–20 (describing the mosaic theory).

69. Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 458–59 (1995) (emphasis omitted) (quoting ALAN WESTIN, *PRIVACY AND FREEDOM* 7 (1967)); see also Francesca Bignami, *Towards a Right to Privacy in Transnational Intelligence Networks*, 28 MICH. J. INT'L L. 663, 669 (2007) (arguing that "when government agencies collect, combine, and manipulate information on individuals without their consent, they breach" the "essential liberal duty" of respecting citizens' choices "to keep certain matters private and to make other matters public").

70. See James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1462 (2004) (explaining that, in certain contexts, "privacy is about control, fairness, and consequences, rather than simply keeping information confidential").

71. See *infra* subpart III(D).

remaining statutory information-sharing limits. The National Security Act of 1947 might prevent the CIA from sharing information with federal law enforcement agencies—most notably the FBI—as well as other counterterrorism officials who operate primarily in the domestic sphere. The Posse Comitatus Act could result in federal criminal liability for members of the Armed Forces who exchange data or otherwise coordinate with law enforcement officials. Finally, the Privacy Act might restrict any federal agency from sharing with intelligence officials unless its reasons for handing over the data are sufficiently similar to the reasons it gathered the information in the first place.⁷²

Each of these statutes reflects a distinct set of policy values. Some laws seek to prevent pretext—the danger that criminal investigators might try to take advantage of the more flexible legal standards that govern surveillance for intelligence purposes. Others reflect firewall concerns; it might be appropriate to use certain military and intelligence practices in the foreign sphere, but those aggressive practices have no place here at home. A third principle is republicanism—the notion that the Armed Forces must always be

72. See *supra* text accompanying note 12. Several other statutes have the potential to restrict information sharing, but do not have that effect at present because of how they are implemented. For instance, the Trade Secrets Act makes it a crime for federal officials to disclose virtually any kind of confidential business information—a restriction that could impede the free flow of data about vulnerabilities at critical infrastructure facilities like chemical plants. See 18 U.S.C. § 1905 (2006) (prohibiting any “officer or employee of the United States” from “publish[ing], divulg[ing], disclos[ing], or mak[ing] known in any manner or to any extent” any “information [that] concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association”). Yet the Trade Secrets Act contains an important exception: it permits disclosures that are otherwise “authorized by law.” *Id.* And the Homeland Security Act of 2002 authorizes intelligence agencies to exchange critical infrastructure information. Pub. L. No. 107-296, §§ 214(e)(1), (2)(D), 116 Stat. 2135, 2154 (codified at 6 U.S.C. §§ 133(e)(1), (2)(D) (2006)). The regulations implementing this directive state that DHS may provide

[Protected Critical Infrastructure Information] to an employee of the Federal government, provided . . . that such information is shared for purposes of securing the critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another appropriate purpose including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to the homeland.

6 C.F.R. § 29.8(b) (2010); see also *Chrysler Corp. v. Brown*, 441 U.S. 281, 312–13 (1979) (holding that validly promulgated regulations can amount to legal authorization within the meaning of the Trade Secrets Act). Similarly, the Health Insurance Portability and Accountability Act of 1996—which Congress enacted to ensure the privacy of personal medical records—conceivably could limit the sharing of information about victims of a bioterrorism attack or a pandemic. See Peter P. Swire & Lauren Steinfield, *Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515, 1525 (2002). However, the HIPAA privacy rule, promulgated by the Department of Health and Human Services in 2000, does not represent much of an obstacle. The privacy rule is understood to regulate only the flow of data from health-care providers to the government, not the flow of data among government agencies. *Id.* at 1528–29. And, in any event, the rule contains a number of exceptions that would permit information sharing in the event of a bioterrorism incident. See, e.g., 45 C.F.R. §§ 164.512(b), (f), (j) (2009) (exceptions for “public health activities,” “law enforcement purposes,” and “avert[ing] a serious threat to health or safety”).

kept firmly under the control of civilian authorities. Finally, there's the good of privacy; the idea is to limit the government's ability to engage in unwanted observation, as well as to respect the data subject's ability to control the manner in which his information is presented to others.

A few qualifications are needed. First, I don't mean to suggest that pretext, firewall, republicanism, and privacy concerns were foremost in Congress's collective mind when it enacted the laws in question. Sometimes they were (the Privacy Act quite obviously was intended to preserve individual privacy), but sometimes they were not (the Posse Comitatus Act in particular comes to mind⁷³). My claim, rather, is that the statutes have the effect of vindicating these values in the present day.

Second, whether or not a given statute prohibits a particular kind of data exchange will rarely be an open-and-shut case. However, the fact that these laws do not unambiguously rule out information sharing is not cause for celebration. Legal uncertainty may be enough to halt data exchange. Risk-averse bureaucrats facing legal commands of unclear meaning may play it safe because they fear that a statutory violation—or even an allegation that a statute has been violated—will result in significant harms.⁷⁴ Officers who share information in violation of the law can expose themselves and their agencies to civil fines and even jail time. Statutory violations can produce less tangible harms as well. Public knowledge that an agency has violated its statutory charter can demoralize employees, decreasing their productivity. It can render the agency politically radioactive, resulting in the President and other senior policy makers keeping it at arm's length. And it can encourage bureaucratic rivals to poach a weakened agency's turf.⁷⁵ In short, it doesn't take a clear prohibition to gum up the works; information sharing can be thwarted nearly as easily by ambiguous legal commands that inspire risk-averse officials to shy away from the legal limits.

A. *The Life and Times of the FISA Wall*

The most notorious wall traces its roots to an obscure provision in FISA.⁷⁶ Enacted in 1978 against the backdrop of the Church Committee's

73. See *infra* notes 151–53 and accompanying text.

74. See MARKLE FOUND., *supra* note 51, at 32 (arguing that information-sharing guidelines must mitigate intelligence officials' risk aversion).

75. Some of these harms may have befallen the CIA in the wake of allegations that the Agency violated domestic and international laws against torture when it subjected al Qaeda leaders to coercive interrogations, including waterboarding. The CIA lost some of its pull with the White House—witness the administration's decision, over CIA objections, to release Justice Department memoranda on the legality of coercive interrogation. Mark Mazzetti & Scott Shane, *Memos Spell Out Brutal C.I.A. Mode of Interrogation*, N.Y. TIMES, Apr. 17, 2009, at A1. And the CIA's responsibility for interrogating senior al Qaeda captives was reassigned to the interagency High-Value Detainee Interrogation Group, or "HIG," which is led by the FBI. Anne E. Kornblut, *New Unit to Question Key Terror Subjects*, WASH. POST, Aug. 24, 2009, at A1.

76. For a detailed history of the FISA wall, see, for example, 9/11 COMMISSION REPORT, *supra* note 2, at 78–80; Kris, *supra* note 3, at 499–518.

explosive allegations of illegal wiretaps, suppression of dissent, and other systematic abuses in the Intelligence Community, FISA put an end to the Executive Branch's practice of conducting national security surveillance unilaterally. Henceforth the executive would need to apply to a special tribunal, known as the FISA Court or FISC, and establish to a judge's satisfaction that surveillance was legally justified.⁷⁷ Among various requirements, FISA directed the government to certify to the court that the "purpose" of the proposed surveillance was to gather foreign intelligence.⁷⁸ The basic idea was that if the government's central aim was to protect against foreign threats, it could avail itself of FISA's relatively lax surveillance standards.⁷⁹ If, on the other hand, the government's objective was principally to enforce domestic criminal laws, it would have to satisfy the relatively strict standards that govern garden-variety criminal investigations.⁸⁰ At some point in the 1980s, the Department of Justice (DOJ) began to read FISA as requiring that "the primary purpose" of the proposed surveillance must be to collect foreign intelligence.⁸¹ (The source of that test was the Fourth Circuit's decision in a pre-FISA case holding that warrantless electronic surveillance is permissible under the Fourth Amendment so long as its primary purpose is to gather foreign intelligence.⁸²)

How did one determine the government's purpose in a given case? By measuring the amount of coordination between intelligence officials and their law enforcement counterparts.⁸³ The more information that changed hands between cops and spies, the more likely it was that the FISA Court would deem the primary purpose of the investigation to be something other than collecting foreign intelligence.⁸⁴ And that would take FISA's relatively liberal surveillance tools off the table.

In 1995, the Justice Department made it official; the agency issued a pair of directives that effectively segregated FBI intelligence officials from criminal investigators at the Bureau and at Main Justice.⁸⁵ The aim of the

77. See 50 U.S.C. § 1804 (2006) (establishing procedures for judicial orders approving electronic surveillance).

78. See *id.* § 1804(a)(7)(B).

79. See *In re Sealed Case*, 310 F.3d 717, 724–25 (FISA Ct. Rev. 2002) (analyzing the legislative history of FISA and highlighting the possibility that intelligence gathering and law enforcement may overlap in certain areas).

80. See *id.* at 725 (noting that "Congress was concerned about the government's use of FISA surveillance to obtain information not truly intertwined with the government's efforts to protect against threats from foreign powers").

81. See *id.* at 722 (discussing the development of the primary purpose test).

82. *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980).

83. Kris, *supra* note 3, at 499–501.

84. *Id.* at 497–99.

85. See, e.g., Memorandum from Jamie S. Gorelick, Deputy Attorney Gen., to Mary Jo White, U.S. Attorney, S. Dist. N.Y. et al. 2 [hereinafter Gorelick Memo], available at <http://www.cnss.org/1995%20Gorelick%20Memo.pdf>; Memorandum from Janet Reno, Attorney Gen., to Assistant Attorney Gen. et al. § (A)(6) (July 19, 1995) [hereinafter Reno Memo], available at <http://www.fas.org/irp/agency/doj/fisa/1995procs.html>.

guidelines was to “clearly separate the counterintelligence investigation from the more limited . . . criminal investigations,” thereby preventing any “unwarranted appearance that FISA is being used to avoid procedural safeguards which would apply in a criminal investigation.”⁸⁶ DOJ therefore directed that information uncovered in the course of intelligence investigations—“including all foreign counterintelligence relating to future terrorist activities”—generally “will not be provided either to the criminal agents, the [U.S. Attorney’s office], or the Criminal Division.”⁸⁷ As a result, information sharing essentially ground to a halt.⁸⁸

The FISA wall thus was not just a statutory restriction; it also derived from administrative and judicial interpretations of the underlying statute. Why was it built in the first place? As the DOJ’s 1995 guidelines indicate, the justification was the need to prevent officials from evading the legal limits on domestic surveillance.⁸⁹ Relatedly, officials wanted to keep the FISA Court from rejecting surveillance applications on the ground that cops’ participation in an intelligence investigation had so contaminated it as to rule out FISA wiretaps.⁹⁰ Let’s call this a pretext concern. (By maintaining the legal limits on domestic surveillance, the FISA wall also sought to preserve the privacy interests of persons subject to surveillance. A good deal more will be said about privacy below.⁹¹)

The risk of pretextual surveillance arises from differences in the respective rules under which intelligence and law enforcement surveillances are carried out. The constitutional and statutory standards that govern the former are weaker than the rules applicable to the latter.⁹² The federal wiretap statute—known in the trade as “Title III”—provides that law enforcement officials generally may not conduct surveillance unless they

86. Gorelick Memo, *supra* note 85, at 2.

87. *Id.* at 2, 3.

88. See *In re Sealed Case*, 310 F.3d 717, 728 (FISA Ct. Rev. 2002) (noting that although the “procedures provided for significant information sharing and coordination . . . , they eventually came to be narrowly interpreted . . . as requiring . . . a ‘wall’ to prevent the FBI intelligence officials from communicating with the Criminal Division regarding ongoing [foreign intelligence] investigations”).

89. See U.S. GEN. ACCOUNTING OFFICE, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED 17 (2001) (explaining that the Reno Memo was designed “to establish a process to properly coordinate DOJ’s criminal and counterintelligence functions and to ensure that intelligence investigations were conducted lawfully”).

90. See *id.* at 12 (discussing FBI officials’ concern that interaction with criminal investigators regarding an intelligence investigation might cause the FISA Court to deny a FISA surveillance application).

91. See *infra* subparts II(D) and III(D).

92. See Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn’t*, 97 NW. U. L. REV. 607, 620 (2003) (comparing the legal thresholds for government surveillance); cf. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 322 (1972) (citing “potential distinctions” between “criminal surveillances and those involving the domestic security”).

obtain a “superwarrant.”⁹³ In addition to showing that they are taking steps to minimize the acquisition of innocent conversations and that they have exhausted alternative investigative techniques, officials must establish probable cause to believe a crime has been, is being, or is about to be committed.⁹⁴ By contrast, FISA only requires intelligence investigators to establish probable cause that the target is a “foreign power” or an “agent of a foreign power”⁹⁵—in layman’s terms, a spy or a terrorist. The standards are looser still for intelligence collection overseas.⁹⁶ The Fourth Amendment may not apply to noncitizens who are not present in the United States—not only the warrant requirement, but also the requirement of reasonableness.⁹⁷ And many surveillance statutes don’t apply to intelligence gathering in foreign countries at all, or at least apply differently than they do here at home.⁹⁸

Those disparate standards create arbitrage opportunities. Officials who are bound by relatively rigorous surveillance rules might look for ways to take advantage of comparatively flabby collection standards. In particular, law enforcement officers might prefer for their wiretaps to be run by counterparts in the Intelligence Community, who would then share the intercepts for use in criminal investigations.⁹⁹ Cops might, in other words, issue tasking orders to spies; they might delegate their responsibilities for criminal surveillance to surrogates in the Intelligence Community. To put matters differently, there could be a substitution effect. If the cost of ordinary criminal surveillance (measured in part by the difficulty of establishing the necessary legal predicates) is excessive, investigators will want to switch to lower cost surveillance techniques. To the extent that intelligence surveillance requires less in the way of predication—a weaker probable cause standard in the domestic sphere, and maybe not even reasonableness in the foreign sphere—law enforcement officials may regard it as a less costly, and therefore more attractive, alternative.

93. Kerr, *supra* note 93, at 645.

94. 18 U.S.C. §§ 2518(3)(a), (3)(c), (5) (2006).

95. 50 U.S.C. §§ 1801(a)–(b), 1805(a)(3) (2006).

96. *See id.* § 1881a(a) (allowing the Attorney General and the Director of National Intelligence to jointly authorize the “targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information”).

97. *See, e.g.,* *United States v. Verdugo-Urquidez*, 494 U.S. 259, 261–65 (1990) (holding that the Fourth Amendment does not extend to searches and seizures of property owned by nonresidents and located in a foreign country). *But cf. Boumediene v. Bush*, 128 S. Ct. 2229, 2255–58 (2008) (establishing a “functional test” to determine whether aliens detained outside of the United States have a constitutional right to seek writs of habeas corpus).

98. James Risen & Eric Lichtblau, *Court Affirms Wiretapping Without Warrants*, N.Y. TIMES, Jan. 16, 2009, at A13.

99. *See Baker, supra* note 25, at 41–42 (describing the temptation for law enforcement officers to recast their investigations as intelligence operations to take advantage of looser standards).

The FISA wall helped prevent this substitution from taking place.¹⁰⁰ The wall effectively increased the cost of the substitute good—law enforcement surveillance conducted by intelligence officials—to infinity; there were no circumstances in which criminal investigators would be permitted to assign to intelligence operatives their responsibility for gathering evidence for use in prosecutions. Notice that the wall didn't just restrict cops from overtly tasking spies with surveillance; it also restricted informal interactions between cops and spies, such as collaborating on overlapping investigations and sharing information with each other.¹⁰¹ The FISA wall thus amounted to a prophylactic rule.¹⁰² In addition to regulating the specific harm that DOJ sought to avert (cops evading the legal limits on domestic surveillance by issuing tasking orders to spies), the wall also proscribed related conduct that could either be wholly innocent or could be the first tentative steps toward an impermissible tasking.¹⁰³

The wall eventually came down. Section 218 of the USA PATRIOT Act abolished the primary purpose test, substituting a new requirement that the government's goal of collecting foreign intelligence must be "a significant purpose" of proposed FISA surveillance.¹⁰⁴ As a result, FISA would still be a viable option even if the government intended to use the resulting intercepts not just to, say, turn a suspected spy into a double agent (a classic counterespionage technique), but also to prosecute that spy for espionage (the textbook law enforcement move).¹⁰⁵ FISA would still be a viable option even if the spies and cops talked to one another about their

100. See Sales, *supra* note 13, at 287–88 (describing how FISA prevented information sharing).

101. *Id.*

102. See, e.g., Brian K. Landsberg, *Safeguarding Constitutional Rights: The Uses and Limits of Prophylactic Rules*, 66 TENN. L. REV. 925, 926 (1999) (describing "prophylactic rules" as "risk-avoidance rules that are not directly sanctioned or required by the Constitution, but that are adopted to ensure that the government follows constitutionally sanctioned or required rules"); David A. Strauss, *The Ubiquity of Prophylactic Rules*, 55 U. CHI. L. REV. 190, 195 (1988) (defining "prophylactic rule" as a "rule that imposes additional requirements beyond those of the Constitution itself").

103. See Sales, *supra* note 13, at 288 (explaining that the FISA Court's requirement that it be informed of all contacts between cops and spies had a chilling effect on their interactions with each other).

104. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (codified at 50 U.S.C. § 1804(a)(6)(B) (2006)). Section 203 of the PATRIOT Act eliminated two other statutory walls. It amended Federal Rule of Criminal Procedure 6(e) to authorize prosecutors to share grand jury information with various national security players, and it amended the federal wiretap statute to authorize criminal investigators to share intercepts with various national security players. See generally Jennifer M. Collins, *And the Walls Came Tumbling Down: Sharing Grand Jury Information with the Intelligence Community Under the USA PATRIOT Act*, 39 AM. CRIM. L. REV. 1261, 1270–86 (2002) (summarizing the changes to Rule 6(e) adopted in the USA PATRIOT Act).

105. Kris, *supra* note 3, at 498 ("[A] FISA wiretap conducted for a law enforcement purpose, such as prosecuting a spy for espionage, would typically be indistinguishable . . . from a FISA wiretap conducted for a traditional intelligence purpose, such as recruiting the spy as a double agent.").

respective approaches to the case.¹⁰⁶ Section 504 was even blunter; it provided that intelligence officials “may consult with Federal law enforcement officers to coordinate efforts” against national security threats.¹⁰⁷ Many academics take a dim view of these changes, arguing that PATRIOT enables officials to engage in what I’m calling pretextual surveillance.¹⁰⁸ The FISA Court shared some of those concerns, but in 2002 the FISA Court of Review upheld the amended FISA against a constitutional challenge.¹⁰⁹

B. *National Security Act of 1947*

The National Security Act of 1947 represents another potentially significant barrier to information sharing. That landmark legislation, enacted in the wake of the Allied victory in World War II and with the Cold War faintly visible on the horizon, established the Central Intelligence Agency,¹¹⁰ granting the Agency certain powers and denying it certain others.¹¹¹ As relevant here, the CIA is denied any “police, subpoena, or law enforcement powers or internal security functions.”¹¹² That notoriously ambiguous prohibition could impede the Agency’s efforts to share intelligence information with counterparts at the FBI or elsewhere in the law enforcement community, and also to receive data from them in return.¹¹³

At least two distinct policy judgments are reflected in the internal security ban. The first might be called a firewall concern. The idea is that,

106. See *In re Sealed Case*, 310 F.3d 717, 734–35 (FISA Ct. Rev. 2002) (explaining that FISA, as amended by the USA PATRIOT Act, allows greater coordination between intelligence and law enforcement officials).

107. USA PATRIOT Act § 504.

108. See, e.g., Banks, *supra* note 37, at 1149 (“As it now stands, the government may take advantage of the secretive and less protective procedures of FISA to plan and carry out surveillance and searches of American citizens, without giving notice or conducting any proceeding before a magistrate.”); Erwin Chemerinsky, *Losing Liberties: Applying a Foreign Intelligence Model to Domestic Law Enforcement*, 51 UCLA L. REV. 1619, 1624 (2004) (“Already it is apparent that the federal government is using its powers under the Patriot Act in contexts that have nothing to do with terrorism.”); David Hardin, *The Fuss over Two Small Words: The Unconstitutionality of the USA Patriot Act Amendments to FISA Under the Fourth Amendment*, 71 GEO. WASH. L. REV. 291, 294 (2003) (arguing that “the new standard serves as an invitation for any proclivity that law enforcement authorities may have in abusing its surveillance authority under the guise of national security while diminishing the judiciary’s role in safeguarding personal rights against unreasonable law enforcement activity”); George P. Varghese, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385, 386 (2003) (calling into question the constitutionality of the PATRIOT Act’s “significant purpose” test).

109. *In re Sealed Case*, 310 F.3d at 746.

110. 50 U.S.C. § 403-4 (2006).

111. The CIA is granted the power to “collect intelligence through human sources and by other appropriate means” but denied any “police, subpoena, or law enforcement powers or internal security functions.” *Id.* § 403-4a(d)(1).

112. *Id.*

113. See Harris, *supra* note 8, at 532–36 (discussing the 1947 Act’s “broad and sometimes vague terms”).

while it might be appropriate for intelligence officials to use aggressive and unsavory techniques overseas, the government should not operate the same way in the domestic sphere.¹¹⁴ Intelligence can be a dirty business. The enterprise involves breaking and entering, theft, eavesdropping on political leaders, kidnapping, unwitting application of mind-altering drugs, coercive interrogations, and the like—sometimes even murder and assassination.¹¹⁵ We might tolerate this sort of state-sanctioned violence if confined to faraway lands (though we might not). But no one thinks it should take place at home. Here, judicial checks on Executive Branch surveillance, seizures, and sanctions are the norm. The internal security ban thus functions as a barrier, preventing the tainted (but perhaps necessary) world of foreign intelligence operations from bleeding over into and contaminating the relatively pristine domestic world.

Commentators often posit that Congress adopted the internal security ban because it wanted to prevent the CIA from emulating the authoritarian German and Soviet intelligence systems.¹¹⁶ Memories of Nazi Germany's notoriously ruthless police force—the Gestapo—were still fresh in 1947. More recent examples could be found behind the descending Iron Curtain, as Stalin began to export his special brand of police terror to his involuntary allies in Central and Eastern Europe.¹¹⁷ The standard account is true enough, but incomplete in one important respect. It doesn't appear that Congress wanted to ban the use of aggressive intelligence techniques *per se*.¹¹⁸ It simply wanted to ban their use *inside the United States*. If Congress had the sweeping ambitions sometimes attributed to it, it could have fortified the CIA's statutory charter with express restrictions on kidnapping, assassination, or numerous other practices. It didn't. Instead, it chose to rule them out in connection with internal security, leaving external security essentially as it found it.¹¹⁹ That suggests Congress may have been content

114. See, e.g., Kate Martin, *Intelligence, Terrorism, and Civil Liberties*, 29 HUM. RTS., Winter 2002, at 5, 5 (arguing that practices that would be dangerously intrusive domestically may be necessary in the war against terrorism).

115. See Roberto Suro, *FBI's "Clean" Team Follows "Dirty" Work of Intelligence*, WASH. POST, Aug. 16, 1999, at A13 (explaining that the FBI uses separate teams to keep more "shocking" tactics confined to the intelligence realm).

116. See, e.g., Sherri J. Conrad, *Executive Order 12,333: "Unleashing" the CIA Violates the Leash Law*, 70 CORNELL L. REV. 968, 975 (1985) (discussing concerns that the CIA may "evolve into an American secret police"); Harris, *supra* note 8, at 531 (asserting that recent memories of World War II led to Congress carving out clear jurisdictional roles for intelligence agencies); Manget, *supra* note 1, at 416 (citing a "deep uneasiness" around the creation of the CIA); Daniel L. Pines, *The Central Intelligence Agency's "Family Jewels": Legal Then? Legal Now?*, 84 IND. L.J. 637, 640 (2009) (stating that Congress did not want the CIA to become another secret police).

117. See Michael Schwartz, *A Celebration is Haunted by the Ghost of Stalin*, N.Y. TIMES, May 8, 2010, at A9.

118. See Conrad, *supra* note 117, at 937 ("Congress designed the National Security Act to interdict domestic spying.").

119. See S. REP. NO. 94-755, at 56 (1976) (citing intelligence officials' testimony that the internal security restriction "was intended to 'draw the lines very sharply between the [Central

to give the CIA relatively free rein to operate overseas. Congress didn't care if the CIA was a "rogue elephant,"¹²⁰ as long as it was stampeding America's enemies rather than her citizens.

The ban on internal security functions serves a second policy value as well—preventing government officials from doing an end run around legal limits on domestic surveillance. This is identical to the FISA wall's *pretext* rationale discussed above.¹²¹ (Again, this anti-pretext provision also preserves the privacy interests of persons subject to surveillance. A good deal more will be said about privacy below.¹²²) If the CIA had internal security responsibilities, investigators might engage in pretextual surveillance—i.e., wiretaps whose superficial purpose is to collect information for intelligence purposes, but whose true objective is to gather evidence for use in a garden-variety criminal investigation. The internal security prohibition makes it harder for law enforcement officials to commission pretextual wiretaps. Because the CIA is statutorily barred from undertaking certain kinds of domestic operations, and perhaps even from sharing information concerning certain domestic operations, there are fewer opportunities for officials to evade the restrictive rules that govern criminal investigations.¹²³ (The seal is not watertight; Executive Order 12,333 authorizes the CIA to undertake a variety of domestic operations, such as protecting agency facilities and personnel against various threats.¹²⁴)

How does the 1947 Act give concrete form to these firewall and pretext concerns? Badly. The terms of the statutory prohibition on "police, subpoena, or law enforcement powers or internal security functions"¹²⁵ are notoriously ambiguous. In 1976, the Church Committee criticized the phrase's indeterminacy.¹²⁶ Modern observers haven't been much kinder. One scholar berates Congress for "failing to use clear and unambiguous language restricting internal operations by the CIA,"¹²⁷ and even the

Intelligence Group] and the FBI" and that the "CIA would be limited definitely to purposes outside of the country").

120. See Editorial, *Let Congress Chain This Rogue Elephant*, DAYTONA BEACH MORNING J., Sept. 12, 1975, at 4A (reporting that Senator Frank Church called the CIA a "'rogue elephant' on a rampage without command").

121. See *supra* notes 90–110 and accompanying text.

122. See *infra* subparts II(D) and III(D).

123. See 50 U.S.C. §§ 401a(1), 403-4a(d) (2006) (limiting the breadth of CIA activities to foreign intelligence and counterintelligence).

124. Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 23, 2003), Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008), *reprinted as amended in* 50 U.S.C. § 401 (2006).

125. 50 U.S.C. § 403-4a(d)(1).

126. See FINAL REPORT OF THE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, S. REP. NO. 94-755, at 96–98 (1976) (referring to the phrase's "ambiguity").

127. Conrad, *supra* note 117, at 971.

Agency's former general counsel confesses that "'the limits of what the CIA can and cannot do are not clear.'"¹²⁸ Nor has the judiciary offered much assistance; "[c]ourts have generally eschewed clear definitions and parameters on CIA domestic activity."¹²⁹ Because of its indeterminacy, the 1947 Act is amenable to any number of competing interpretations. A strict reading of "internal security," championed by some,¹³⁰ would exclude the CIA from virtually any domestic responsibilities whatsoever.¹³¹ The flexible reading favored by others¹³² would preserve at least some domestic responsibilities for the agency.

Who's right? The answer matters a great deal. Depending on how it is interpreted, the internal security ban could impose severe restrictions on information sharing between the CIA and the FBI and other domestic entities.¹³³ To be sure, the Agency and Bureau don't need a statute to keep them from swapping data; as bitter bureaucratic rivals, they will have strong incentives to keep their information to themselves.¹³⁴ Yet legal restrictions can make matters worse.

For instance, the 1947 Act conceivably could prevent the FBI and CIA from mounting joint investigations of global terrorist groups. Imagine a terrorist outfit whose members are based overseas but who occasionally travel to the United States to raise money, case targets, and conduct operations; the group has both a domestic and an international presence. The Bureau and Agency might want to divide the labor: the CIA would surveil targets when they are abroad, the FBI would surveil any targets who happen to be within the United States, and they would hand off the baton as targets cross the border. The two agencies then would share their respective surveillance take with each other. (This is an example of how information sharing can reduce the need for redundant collection efforts, thereby promoting efficiency.) The 1947 Act might forbid the data exchange on which this sort of collaboration depends.

Consider the flow of information from the CIA to the FBI. The FBI isn't just responsible for domestic intelligence; it's also the nation's

128. Harris, *supra* note 8, at 533 (quoting Jeffrey H. Smith, former CIA general counsel).

129. *Id.* at 534.

130. See, e.g., Conrad, *supra* note 117, at 973 & n.35, 975–76 (discussing how certain courts interpret the phrase "internal-security functions in a restrictive manner").

131. See *id.* at 972–73 n.35 (criticizing Executive Order 12,333's interpretation of the phrase "internal security" and arguing that "Congress prohibited all CIA domestic activity except for matters of CIA facility security and personnel").

132. See Harris, *supra* note 8, at 547 (discussing how the Act's ambiguity gives rise to flexible interpretations).

133. See Conrad, *supra* note 117, at 988 (arguing that the 1947 Act restricts the CIA from exchanging data with domestic entities).

134. See Sales, *supra* note 13, at 303–13.

preeminent law enforcement agency.¹³⁵ That means the Bureau may want to use a given piece of information for intelligence purposes, but it also may want to use the same data in criminal proceedings; the information is “dual use.”¹³⁶ Suppose the CIA hands the FBI intelligence information that it collected overseas. If the Bureau intends to use it in a criminal prosecution, the CIA becomes an active participant in the collection of evidence for use at trial.¹³⁷ The CIA effectively operates as the FBI’s agent, exercising something like a delegated power to collect evidence of criminal activity. Does that count as the exercise of a “law enforcement power[.]” within the meaning of the 1947 Act? The case that it does is by no means frivolous. Similar problems are evident when information flows in the opposite direction. May the Bureau give the CIA its dual-use information—i.e., data that was gathered partly for law enforcement purposes? The CIA’s receipt of the data makes it a direct beneficiary of a core law enforcement function—collecting evidence of criminal wrongdoing—and that could be seen as participation in the exercise of a “law enforcement power[.]”¹³⁸

Even worse, the FBI’s intentions may not be clear, and they may evolve over time. This is in essence a retroactivity problem. At the moment the CIA and the Bureau swap information; the two agencies may intend for it to be used only for intelligence purposes. But at some point the FBI might decide that the most effective way to proceed against a particular terrorist is to charge him with a crime. The guidelines that govern FBI operations recognize that these categories are fluid:

[T]he FBI’s information gathering activities [need not] be differentially labeled as “criminal investigations,” “national security investigations,” or “foreign intelligence collections,” or that the categories of FBI personnel who carry out investigations be segregated from each other based on the subject areas in which they operate. Rather, all of the FBI’s legal authorities are available for deployment in all cases to which they apply to protect the public from crimes and threats to the national security and to further the United States’ foreign intelligence objectives.¹³⁹

135. *New Attorney General Guidelines for Domestic Intelligence Collection: Hearing Before the S. Comm. on Intelligence*, 110th Cong. 1 (2008) (joint statement of Elisebeth Collins Cook, Assistant Att’y Gen. of the Office of Legal Policy, and Valerie Caproni, Gen. Counsel of the FBI).

136. See Michael B. Mukasey, *Where the U.S. Went Wrong on the Christmas Day Bomber*, WASHINGTONPOST.COM, Feb. 12, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/11/AR2010021103331.html> (explaining that the FBI seeks to protect the public from crimes and threats to national security, and to further foreign intelligence objectives).

137. Depending on the arrangement, the FBI might be barred from using CIA-originated information in criminal proceedings without the Agency’s permission. Information-sharing agreements between agencies (or between nations) often include ORCON restrictions—that is, “originator controls”—that bar recipients from using the data in particular ways unless the originator consents. See LOWENTHAL, *supra* note 24, at 154.

138. 50 U.S.C. § 403-4a(d)(1) (2006).

139. THE ATTORNEY GENERAL’S GUIDELINES FOR DOMESTIC FBI OPERATIONS 7 (2008).

An investigation that began life looking like an intelligence matter could reach maturity looking like a criminal matter, and vice versa. As a result, data exchange that was entirely unrelated to the criminal law when it took place could be retroactively converted, thanks to the FBI's latter-day shift in emphasis, into law enforcement activity that violates the 1947 Act.

The National Security Act could impede sharing in another way, too: by preventing the CIA from participating in operations to capture suspected terrorists abroad and bring them to the United States to stand trial. The Agency sometimes apprehends terrorists and others wanted by the FBI.¹⁴⁰ In the late 1990s, the CIA crafted a plan to kidnap Osama Bin Laden in Afghanistan; the Saudi was under indictment in the Southern District of New York for al Qaeda's 1998 bombing of two American embassies in East Africa, and a CIA snatch job would be the first step in bringing the terror master to justice.¹⁴¹ The CIA taking Bin Laden into custody might count as "law enforcement" within the meaning of the 1947 Act: the Agency essentially would be functioning as the FBI's delegate, performing the core law enforcement function of apprehending a fugitive so he can be brought before a court.¹⁴² The 1947 Act similarly might rule out information sharing about such apprehensions. Suppose the FBI itself captures Bin Laden after being tipped off by CIA analysts that he is hiding out at his Tarnak Farms compound in Afghanistan. Is it law enforcement for the CIA to share information it knows the FBI will use in connection with a criminal prosecution? What if, at the time of the capture, the government hasn't decided what it will do with Bin Laden once he's in custody? Criminal prosecution is an obvious option, but it's not the only one; Bin Laden might be held in military custody or held by the CIA for interrogation. Does the mere possibility of criminal proceedings convert the CIA's information sharing into "law enforcement" in violation of the 1947 Act?¹⁴³

140. See David Stout, *C.I.A. Detainees Sent to Guantánamo*, NYTIMES.COM, Sept. 6, 2006, <http://www.nytimes.com/2006/09/06/washington/06cnd-bush.html> (describing the CIA's apprehension program).

141. See WRIGHT, *supra* note 2, at 265–66 (detailing a CIA plan to use Afghan tribesmen—who were leftover assets from the conflict with the Soviets—to kidnap Bin Laden, and describing the evidence used in the New York grand jury indictment).

142. See LOWENTHAL, *supra* note 24, at 188 (noting that renditions "require the presence of U.S. law enforcement personnel even if the operation is primarily an intelligence operation").

143. Section 905 of the USA PATRIOT Act might permit some of these information-sharing initiatives, but it isn't a slam dunk. The statute amends the 1947 Act by generally providing that the Attorney General, or the head of any other department or agency of the Federal Government with law enforcement responsibilities, shall expeditiously disclose to the Director of Central Intelligence . . . foreign intelligence acquired by an element of the Department of Justice or an element of such department or agency, as the case may be, in the course of a criminal investigation.

USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 905, 115 Stat. 272, 388–89 (codified at 50 U.S.C. § 403-5b, 5c (2006)). But § 905 has its limits. First, it doesn't authorize bilateral data exchange; it only permits sharing in one direction, from the law enforcement world to the CIA. See *id.* (requiring law enforcement agencies to disclose foreign intelligence to the CIA, but remaining

Again, the point is not that the CIA's statutory charter clearly rules out these sorts of information-sharing arrangements. It doesn't. The scope of the ban on "police, subpoena, or law enforcement powers or internal security functions"¹⁴⁴ is not a model of clarity, and it's far from certain which types of data exchange are permitted and which are forbidden. But that is not a point in the statute's favor. Mere ambiguity can be enough to dissuade government officials from sharing information with one another, as they worry about whether doing so would land their agencies—or themselves—in hot water.

C. *Posse Comitatus Act*

The Posse Comitatus Act is a second possible source of information-sharing limits. Originally enacted in 1878, the Act makes it a crime for anyone "willfully [to] use[] any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws" except "in cases and under circumstances expressly authorized by the Constitution or Act of Congress."¹⁴⁵ *Posse comitatus* refers to the common law power of a sheriff to "summon [t]he entire population of a county above the age of 15 . . . as to aid him in keeping the peace, in pursuing and arresting felons."¹⁴⁶ The Posse Comitatus Act is one of the more venerated laws in the U.S. Code. It's also one of the more vexing, because its strict but ambiguous limits could interfere with information sharing between law enforcement authorities and the Armed Forces.¹⁴⁷

The Posse Comitatus Act vindicates two distinct policy values. The first is the familiar firewall concern—the notion that some national security operations ought not to be attempted in certain contexts even if they're unobjectionable elsewhere.¹⁴⁸ The second might be called a republicanism concern—i.e., the longstanding American determination to preserve representative self-government, in part by securing civilian control of the Armed Forces.¹⁴⁹ I do not argue that firewall and republicanism values were at the top of Congress's list of priorities when it passed the Posse Comitatus Act. To the contrary, the historical evidence suggests that the Reconstruction

silent on information transfer from the CIA to law enforcement agencies). It therefore wouldn't override any restriction in the 1947 Act on the CIA sending information to counterparts at law enforcement agencies. Second, and more importantly, § 905 only permits sharing "[e]xcept as otherwise prohibited by law." *Id.* That reservation clause might maintain any information-sharing limits required by CIA's statutory charter.

144. 50 U.S.C. § 403-4a(d)(1).

145. 18 U.S.C. § 1385 (2006).

146. DELUXE BLACK'S LAW DICTIONARY 1162 (6th ed. 1990); *see also* BLACK'S LAW DICTIONARY 1183 (8th ed. 2004) (defining *posse comitatus* as a "group of citizens who are called together to help the sheriff keep the peace or conduct rescue operations").

147. *See* Sales, *supra* note 13, at 329.

148. *See supra* notes 115–31 and accompanying text.

149. *See* THE FEDERALIST NO. 8, at 67–70 (Alexander Hamilton) (Clinton Rossiter ed., 1961) (expressing concern that maintaining a large standing army can lead to oppression).

Congress enacted the legislation for odiously racist reasons.¹⁵⁰ The states of the former Confederacy objected to the use of federal troops to guarantee freedmen the right to vote and generally to prevent election fraud.¹⁵¹ In 1878 they managed to persuade the rest of Congress to enact their preferences into law.¹⁵² Whatever its origins, however, the Posse Comitatus Act today has come to stand for these two policy concerns.

Consider firewall principles first. The Posse Comitatus Act reflects the notion that the Armed Forces—more precisely, the Army and the Air Force (the Act doesn't mention the Navy or Marines, though the Defense Department applies it to them as a matter of policy¹⁵³)—should be kept separate from the world of law enforcement.¹⁵⁴ The Act thus serves to insulate criminal investigations from the more violent practices and rules of engagement that characterize military operations.¹⁵⁵ This firewall concern is similar to the rationale for Congress's decision in the National Security Act of 1947 to largely exclude the CIA from domestic operations.¹⁵⁶ But there is a subtle difference. The 1947 Act draws both a geographic line of demarcation (the CIA may operate overseas but not in the United States) and a functional one (the CIA may engage in intelligence but not law enforcement).¹⁵⁷ Posse Comitatus, by contrast, draws only a functional line. The Armed Forces may undertake military functions but they may not assume law enforcement responsibilities.¹⁵⁸

150. See, e.g., Gary Felicetti & John Luce, *The Posse Comitatus Act: Setting the Record Straight on 124 Years of Mischief and Misunderstanding Before Any More Damage Is Done*, 175 MIL. L. REV. 86, 90 (2003) (citing “the Act’s true origins in Reconstruction bitterness and racial hatred”).

151. *Id.* at 110.

152. See, e.g., Candidus Dougherty, “Necessity Hath No Law”: *Executive Power and the Posse Comitatus Act*, 31 CAMPBELL L. REV. 1, 12–14 (2008) (describing the long tension between southern states and Congress regarding freedmen’s rights, influencing the 1876 presidential election and resulting in passage of the Posse Comitatus Act in 1878); Felicetti & Luce, *supra* note 151, at 100–13.

153. See Michael Greenberger, *Did the Founding Fathers Do “A Heckuva Job”?* *Constitutional Authorization for the Use of Federal Troops to Prevent the Loss of a Major American City*, 87 B.U. L. REV. 397, 406 (2007).

154. See Felicetti & Luce, *supra* note 151, at 120 (citing a unanimous 1882 Senate Judiciary Committee report confirming the “primary evil addressed by the Posse Comitatus Act [as] the marshal’s power to call out and control the Army”).

155. *Effect of Posse Comitatus Act on Proposed Detail of Civilian Employee to the National Infrastructure Protection Center*, Memorandum from William Michael Treanor, Deputy Assistant Att’y Gen., Office of Legal Counsel, to the General Counsel, FBI (May 26, 1998), available at <http://www.justice.gov/olc/pca1fnl.htm> (“Relevant caselaw and opinions of [the Office of Legal Counsel] reflect the view that the PCA is intended to prohibit military personnel from directly coercing, threatening to coerce, or otherwise regulating civilians in the execution of criminal or civil laws.”).

156. See *supra* note 114 and accompanying text.

157. See *supra* note 114 and accompanying text.

158. See *supra* note 146 and accompanying text.

The underlying insight is that soldiers and cops have fundamentally different missions. The soldier's job is to kill the enemy; the cop's is to enforce the law.¹⁵⁹ The military subdues enemy forces through overwhelming violence.¹⁶⁰ Law enforcement doesn't have "enemies"; instead, officers encounter presumptively innocent fellow citizens who are entitled to a full panoply of constitutional rights, both substantive and procedural.¹⁶¹ Another important difference has to do with the permissibility of force. The default rule for soldiers on the battlefield is that they are entitled to use force, even deadly force.¹⁶² The default rule for cops on the beat is the opposite; they may use deadly force only in extreme circumstances, as when a suspect threatens the life of a police officer or a bystander.¹⁶³ Battlefield rules of engagement seek to maximize military effectiveness;¹⁶⁴ the rules governing criminal investigations seek to constrain, to prevent officers from investigating, arresting, and detaining too aggressively.¹⁶⁵ The Posse Comitatus Act thus prevents military mores and practices—which are entirely justified on the battlefield—from contaminating the separate world of civilian law enforcement with its very different priorities and balancing of equities.

The firewall's benefits run in both directions. Keeping soldiers from enforcing the law doesn't just protect civilians, it also protects the military. If the Armed Forces assume routine law enforcement responsibilities, their scarce resources—financial, equipment, personnel, and otherwise—will be diverted away from their core mission of fighting wars.¹⁶⁶ There is also a more immediate risk that law enforcement responsibilities will blunt the

159. See DIANE CECILIA WEBER, CATO INST., WARRIOR COPS: THE OMINOUS GROWTH OF PARAMILITARISM IN AMERICAN POLICE DEPARTMENTS 10 (1999); William C. Banks, *The Normalization of Homeland Security After 9/11: The Role of the Military in Counterterrorism Preparedness and Response*, 64 LA. L. REV. 735, 771 (2004); Sean J. Kealy, *Reexamining the Posse Comitatus Act: Toward a Right to Civil Law Enforcement*, 21 YALE L. & POL'Y REV. 383, 386 (2003) (explaining crucial differences between military objectives and law enforcement objectives).

160. See WEBER, *supra* note 160, at 3 ("In boot camp, recruits are trained to inflict *maximum* damage on enemy personnel.").

161. See, e.g., Banks, *supra* note 160, at 771; Kealy, *supra* note 160, at 386.

162. See WEBER, *supra* note 160, at 10 ("The soldier confronts an enemy in a life-or-death situation" and therefore "learns to use lethal force on the enemy, both uniformed and civilian, irrespective of age or gender."). *But see id.* at 9 (noting that "[i]n the military's newest 'peacekeeping' role abroad, it is obliged—much as civilian police—to be 'highly discreet when applying force'").

163. See, e.g., *Tennessee v. Garner*, 471 U.S. 1, 11 (1985) (declaring unconstitutional a state statute permitting police to use deadly force to apprehend nonviolent fleeing suspects).

164. Mark J. Osiel, *Obeying Orders: Atrocity, Military Discipline, and the Law of War*, 86 CAL. L. REV. 939, 1114 (1998).

165. See Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEXAS L. REV. 49, 49–50 (1995) (discussing how the Fourth Amendment privacy protections restrain law enforcement activities).

166. See Kealy, *supra* note 159, at 402–21 (arguing that diversion of military resources can hinder military preparedness).

military's combat readiness.¹⁶⁷ In training for and performing police functions, soldiers may begin to acquire some of the institutional cop culture of caution and scrupulous legalism. And that could come at the cost of military effectiveness. "If military personnel are trained to overcome their 'shoot to kill' orientation, they may sacrifice their sharpness as soldiers."¹⁶⁸

The second value served by the Posse Comitatus Act is republicanism. The Act reinforces America's basic commitment to representative self-government and its concomitant aversion to military rule.¹⁶⁹ The founding generation's apprehensions about standing armies are well known and needn't be rehearsed at length here.¹⁷⁰ For John Adams, the Boston Massacre was the inevitable result of the Crown's decision to station Redcoats in the city center and charge them with enforcing civil laws: "[S]oldiers quartered in a populous town, will always occasion two mobs, where they prevent one.—They are wretched conservators of the peace!"¹⁷¹ A more specific formulation of this concern is that the military shouldn't wield any influence in civilian matters; the Supreme Court has averted to the "traditional and strong resistance of Americans to any military intrusion into civilian affairs."¹⁷² More specific still is the principle that the military should play no role in the enforcement of civil laws.¹⁷³

Posse Comitatus helps promote the republican value of self-government by reducing the likelihood that civilian authorities will lose control over the military. The Act excludes the Armed Forces from making even minimal

167. See Banks, *supra* note 159, at 771.

168. *Id.*

169. See *supra* note 150 and accompanying text.

170. See, e.g., Nathan Canestaro, *Homeland Defense: Another Nail in the Coffin for Posse Comitatus*, 12 WASH. U. J.L. & POL'Y 99, 105 (discussing American colonists' view of standing armies as instruments of oppression and tyranny); Dougherty, *supra* note 152, at 4–8 (chronicling the Founders' fear of standing armies); Kealy, *supra* note 159, at 391 (recounting the Founders' arguments against standing armies).

171. John Adams, Argument, in 3 LEGAL PAPERS OF JOHN ADAMS 266 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965).

172. *Laird v. Tatum*, 408 U.S. 1, 15 (1972); see also Banks, *supra* note 159, at 740 (describing the Posse Comitatus Act as "[t]he most concrete manifestation of the American tradition of keeping the military out of domestic civilian affairs"); Scott R. Tkacz, *In Katrina's Wake: Rethinking the Military's Role in Domestic Emergencies*, 15 WM. & MARY BILL RTS. J. 301, 307 (2006) (explaining that Posse Comitatus "reaffirm[s] the deeply held American principle that civilian and military spheres should be kept distinctly separate"). But see Felicetti & Luce, *supra* note 150, at 93 ("While the nation's founders were deeply concerned with the abuses of the British Army during the colonial period and military interference in civil affairs, the majority was even more concerned about a weak national government incapable of securing life, liberty, and property." (footnotes omitted)).

173. See Banks, *supra* note 159, at 741 (calling the Posse Comitatus Act "a symbol of our nation's . . . distaste of military involvement in domestic law enforcement"); Canestaro, *supra* note 171, at 99 (explaining that the Act upholds "a basic value of American democracy—the principle that the military cannot enforce civilian law"); Roger Blake Hohnsbeen, *Fourth Amendment and Posse Comitatus Act Restrictions on Military Involvement in Civil Law Enforcement*, 54 GEO. WASH. L. REV. 404, 404 (1986) ("It is a strong tradition in the United States to eschew the use of military force in the routine enforcement of civil laws.").

inroads into the world of civilian law enforcement for fear that such a beachhead could eventually cause the military to gain a measure of independence—or even lead to outright military rule. In other words, the Act aims at preventing the nation from taking the first, tentative steps down a slippery slope toward a coup. It's jarring to read those words. Today, two centuries into the American experiment, with our tradition of civilian control of the military firmly established, the chances that the Armed Forces might take control of the government are vanishingly small, probably even nonexistent.¹⁷⁴ But in 1878, with memories of the Civil War and its attendant military courts, military governors, and other incidents of military rule still fresh, anxieties about the long run viability of republican self-government must have been acute.

The Act helps preserve republicanism in a second, more practical, way. It keeps the military from exerting undue influence in domestic policy debates. The general public—and, derivatively, elected officials—might defer to the Armed Forces because of the stratospherically high esteem in which they are held. In a June 2009 Gallup poll, fully 82% of adults reported having “a great deal” or “quite a lot” of confidence in the military.¹⁷⁵ The military scored 15 points higher than the next most popular choice (small business, weighing in at 67%), and it trounced such also-rans as the presidency (51%), the Supreme Court (39%), and Congress (17%!).¹⁷⁶ It is conceivable that some citizens might embrace the Armed Forces' policy views, not so much because they independently conclude that those preferences are sound, but because their respect for soldiers is so great that they are simply willing to take the military's word for it. The Posse Comitatus Act helps prevent that preference substitution by keeping the military from forming (at least some) domestic policy preferences in the first place.¹⁷⁷ That is, the Act keeps the military from developing an institutional perspective on the law enforcement issues it demarcates as out of bounds. Voters and civilian political leaders thus remain relatively free to deliberate over questions of domestic law enforcement policy without deferring excessively to the military's preferences.

The Posse Comitatus Act gives concrete form to these general principles through a deceptively simple directive:

174. See Canestaro, *supra* note 170, at 140 (“The military would rightfully contest any suggestion that their soldiers would either undermine American values or subvert our democracy.”); *id.* at 139 (citing the “dissipation of the fear that Americans have historically harbored towards a standing army”).

175. Lydia Saad, *Americans' Confidence in Military Up, Banks Down*, GALLUP.COM, June 24, 2009, <http://www.gallup.com/poll/121214/americans-confidence-military-banks-down.aspx>.

176. *Id.*

177. See Banks, *supra* note 159, at 740 (describing the Posse Comitatus Act as “[t]he most concrete manifestation of the American tradition of keeping the military out of domestic civilian affairs”).

Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.¹⁷⁸

That sounds simple enough, but in practice the Act is plagued by ambiguity.¹⁷⁹ Some commentators say the Act bars a fairly wide range of conduct,¹⁸⁰ while others think it doesn't rule out much at all.¹⁸¹ How to construe the Act is of more than academic interest, however, because criminal penalties await those who violate it.¹⁸² No one has ever been prosecuted under the Act,¹⁸³ but uncertainty about its scope and the mere threat of criminal sanctions can deter military officials from taking actions that may well be lawful.

Of particular interest here, it remains unclear to what extent Posse Comitatus allows law enforcement officials and military officers to share information with one another.¹⁸⁴ Indeed, in part because of the Act, military brass appear to be exceedingly reluctant to share information with their colleagues in law enforcement agencies.¹⁸⁵ A series of hypotheticals should help illustrate why.

Imagine that al Qaeda carries out a catastrophic terrorist attack in the United States—say a cell of operatives detonates explosives at a Midwestern shopping mall during the Christmas rush, collapsing the structure and killing hundreds of shoppers. The FBI will play a leading role in the investigation, and it may want to use various military assets. For instance, the Bureau

178. 18 U.S.C. § 1385 (2006).

179. See James Balcius & Bryan A. Liang, *Public Health Law & Military Medical Assets: Legal Issues in Federalizing National Guard Personnel*, 18 ANNALS HEALTH L. 35, 39 (2009) (describing the Act's "brevity and vagueness"); Linda J. Demaine & Brian Rosen, *Process Dangers of Military Involvement in Civil Law Enforcement: Rectifying the Posse Comitatus Act*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 167, 170 (2005) (explaining that the Act is "riddled with uncertainty and complexity"); Felicetti & Luce, *supra* note 150, at 88 (describing "the confusion surrounding the Posse Comitatus Act"); Tkacz, *supra* note 172, at 309 (arguing that Posse Comitatus "creat[es] uncertainty as to exactly what statutory limits restrict the President in times of emergency").

180. See, e.g., Felicetti & Luce, *supra* note 150, at 153 (noting that the Department of Defense set forth "an extremely broad interpretation" of the Act—it "prohibits all 'direct' DOD participation in law enforcement; civilians should not be subject to military power that is regulatory, proscriptive, or compulsory in nature").

181. See, e.g., Dougherty, *supra* note 152, at 17–18 (arguing that the Act does not limit the President's use of military as law enforcement under the emergency powers doctrine).

182. 18 U.S.C. § 1385.

183. See Kealy, *supra* note 159, at 405.

184. See Gustav Eyler, *Gangs in the Military*, 118 YALE L.J. 696, 717–19 (2009) (discussing the "military's hesitancy to communicate and cooperate fully with civilian law enforcement agencies" because of cautious interpretations of the Posse Comitatus Act).

185. See, e.g., Kealy, *supra* note 159, at 432 (arguing that "the military should not only be allowed, but encouraged, to share information with law enforcement when it is necessary to prevent or investigate criminal activity").

might ask the Pentagon to provide it with overhead imagery of the attack site, either from satellites or from Air Force reconnaissance aircraft; a bird's-eye view of the blast pattern might reveal some clues about the attack's origins. Or it might give samples of explosives residue to the Army for forensic analysis; Army experts might be able to shed some light on the type of materiel used in the attack, where it can be obtained, and even the possible identity of the perpetrators. Or the local FBI field commander might ask a counterpart in the U.S. Northern Command for tactical advice on how to most effectively quarantine the attack site and manage access to the rubble.

May the Armed Forces share this sort of information with the FBI? In other words, does it count as "otherwise . . . execut[ing] the laws"¹⁸⁶ within the meaning of the Posse Comitatus Act for the military to give imagery,¹⁸⁷ forensic analysis, and other types of information to a law enforcement agency like the Bureau? The leading federal cases interpreting the Act—a quartet of decisions arising out of the Wounded Knee Siege in the 1970s—send mixed signals.¹⁸⁸

On February 27, 1973, a group of armed men calling themselves the American Indian Movement seized control of Wounded Knee, a town in the southwest corner of South Dakota.¹⁸⁹ Federal law enforcement and military personnel quickly cordoned off the town, and the two sides maintained an uneasy standoff for seventy-one days, sometimes exchanging gunfire.¹⁹⁰ During the siege, the Armed Forces occasionally passed intelligence information to on-site law enforcement officials (mostly imagery taken from reconnaissance planes); they also offered tactical advice, such as tips on how to end the standoff with a minimum amount of bloodshed.¹⁹¹ A number of the gunmen eventually found themselves in the dock facing a variety of federal criminal charges.¹⁹² The defendants' strategy was to deny that they had committed the crime of interfering with a "law enforcement officer lawfully engaged in the lawful performance of his official duties,"¹⁹³ because

186. 18 U.S.C. § 1385.

187. Cf. Siobhan Ghorman, *White House to Abandon Spy-Satellite Program*, WSJ.COM, June 23, 2009, <http://online.wsj.com/article/SB124572555214540265.html> (recounting concerns that the Posse Comitatus Act is violated by a program that shares military satellite imagery with domestic agencies).

188. See Canestaro, *supra* note 170, at 127–29 (surveying the contradictory interpretations of the Posse Comitatus Act in the litigation following the Wounded Knee Siege); Felicetti & Luce, *supra* note 150, at 145–46 (discussing the "confusing patchwork of decisions" that resulted from the Wounded Knee Siege); Hohnsbeen, *supra* note 173, at 409–13 (summarizing the holdings in the four seemingly contradictory cases).

189. Canestaro, *supra* note 170, at 126.

190. *Id.* at 126–27.

191. Hohnsbeen, *supra* note 173, at 409.

192. *Id.* at 409–10.

193. 18 U.S.C. § 231(a)(3) (2006).

the military's involvement at Wounded Knee violated the Posse Comitatus Act and thus rendered the officers' actions unlawful.¹⁹⁴

Two judges agreed. *United States v. Jaramillo*¹⁹⁵ held that the soldiers had so "perva[sively]" assisted the cops that there was a reasonable doubt whether the latter were lawfully engaged in the lawful performance of their duties.¹⁹⁶ One of the things the *Jaramillo* court cited as an example of impermissible military involvement was giving tactical advice to law enforcement officials—a form of information sharing.¹⁹⁷ Similarly, in *United States v. Banks*,¹⁹⁸ the court found that the totality of the evidence suggested that the military's involvement at Wounded Knee crossed the line into a Posse Comitatus violation (though it did not identify specific acts that offended the statute).¹⁹⁹ Two other judges saw things differently. *United States v. Red Feather*²⁰⁰ held that only the "direct active use" of soldiers to enforce the law violates the Posse Comitatus Act.²⁰¹ Anything short of that—including the military's behind-the-scenes assistance at Wounded Knee—is permissible. Likewise, *United States v. McArthur*²⁰² held that the information sharing and other forms of assistance did not offend the Posse Comitatus Act, because the Armed Forces did not subject citizens to military power that was "regulatory, proscriptive, or compulsory."²⁰³

Given these precedents, may the military share satellite imagery, forensics analysis, tactical advice, and other types of information with the FBI in the wake of a domestic terrorist attack? Under *Jaramillo* and *Banks*, that may well violate Posse Comitatus.²⁰⁴ Under *Red Feather* and *McArthur*, it probably doesn't.²⁰⁵ That uncertainty may be enough to keep the Armed Forces from swapping data with the Bureau; risk-averse officials may decide

194. Canestaro, *supra* note 170, at 127.

195. 380 F. Supp. 1375 (D. Neb. 1974).

196. *Id.* at 1379–81.

197. *Id.* at 1381.

198. 383 F. Supp. 368 (D.S.D. 1974).

199. *See id.* at 375–76 (holding that the evidence did not support a conclusion that the government activity was lawful).

200. 392 F. Supp. 916 (D.S.D. 1975).

201. *See id.* at 923 (discussing the broad authority granted to the military to involve itself indirectly with civilian law enforcement operations).

202. 419 F. Supp. 186 (D.N.D. 1976), *aff'd sub nom.* *United States v. Casper*, 541 F.2d 1275 (8th Cir. 1976).

203. *Id.* at 194–95.

204. *See Banks*, 383 F. Supp. at 375–76 (citing the use of military equipment and tactical consultation with military personnel as an example of conduct that may be impermissible under the Posse Comitatus Act); *United States v. Jaramillo*, 380 F. Supp. 1375, 1381 (D. Neb. 1974) (citing the provision of military advice and information as examples of conduct that may be impermissible under the Posse Comitatus Act).

205. *See McArthur*, 419 F. Supp. at 194 (explaining that a violation of the Posse Comitatus Act requires military action that is "regulatory, proscriptive, or compulsory," which would be beyond mere intelligence sharing); *Red Feather*, 392 F. Supp. at 923 (holding that only "direct active use" of soldiers to enforce the law violates the Posse Comitatus Act).

that the safest bet is to avoid any conduct that even arguably violates the act—especially since a Posse Comitatus violation is a crime that could land one in jail.²⁰⁶

Of course, Congress is free to carve out exceptions to Posse Comitatus, and it has done so on a number of occasions.²⁰⁷ The legality of information sharing is complicated by a 1981 exception intended to promote military cooperation with criminal investigations of narcotics trafficking in the Caribbean;²⁰⁸ it provides that “[t]he Secretary of Defense may . . . provide . . . civilian law enforcement officials any information collected during the normal course of military training or operations.”²⁰⁹ The idea seems to be that the Armed Forces may share intelligence with law enforcement if they just so happen to come across it in the ordinary course of business, but they may not—and this is key—share intelligence they have deliberately set out to collect on law enforcement’s behalf.²¹⁰ The 1981 amendment thus reflects something like the “plain view” doctrine from Fourth Amendment law.²¹¹ Let’s return to our hypothetical attack. It’s unclear whether overhead imagery, forensic analysis, and other intelligence provided by the Armed Forces to the FBI would count as “collected during the normal course of military training or operations.”²¹² In this scenario, as is likely to be the case in the real world, the military is actively partnering with law enforcement. The cops are not mere passive recipients of whatever the military chooses to send them; they are collaborating to ensure that military collection meets the FBI’s needs. That active role for law enforcement in determining the Armed Forces’ intelligence activities may remove the resulting intelligence take from the murky category of “normal . . . military operations”²¹³ and place it squarely in the realm of “otherwise . . . execut[ing] the laws.”²¹⁴

206. See *supra* note 75 and accompanying text.

207. See, e.g., 10 U.S.C. § 332 (2006) (authorizing the President to use the Armed Forces to put down “unlawful obstructions, combinations, or assemblages, or rebellion against the authority of the United States,” when it is “impracticable to enforce the laws of the United States in any state by the ordinary course of judicial proceedings”).

208. See Hohnsbeen, *supra* note 173, at 416–19.

209. 10 U.S.C. § 371(a) (2006).

210. For instance, the House Report discussing the 1981 amendment suggests that “the scheduling of routine training missions can easily accommodate the need for improved intelligence information concerning drug trafficking in the Caribbean.” H.R. REP. NO. 97-71, pt.2, at 8 (1981); see also Hohnsbeen, *supra* note 173, at 422 (speculating that “the military could alter its normal course of operations to accommodate civilian needs”). In practical terms, this would mean that the Air Force may not fly reconnaissance missions whose express purpose is to surveil offshore drug smugglers. But it would be permissible to inform the cops if a routine training flight happens to find evidence of narcotics trafficking. And it would be permissible to schedule routine training flights in the hopes that such evidence will be uncovered.

211. See, e.g., *Arizona v. Hicks*, 480 U.S. 321 (1987).

212. 10 U.S.C. § 371(a).

213. *Id.*

214. 18 U.S.C. § 1385 (2006).

Even more vexing line-drawing problems can arise. Consider the complications that result from the fact that the FBI is a hybrid entity that combines both law enforcement responsibilities and domestic intelligence functions.²¹⁵ Roughly speaking, the Bureau has two options for how to handle our hypothetical mall bombing: through a criminal investigation or an intelligence investigation.²¹⁶ Which tack the FBI takes could make a big difference to the Posse Comitatus analysis. If the Armed Forces share information with Bureau personnel who are treating the attack primarily as an intelligence matter, the Act's strictures may not be implicated.²¹⁷ But what if the military shares the very same information with the very same FBI personnel when the latter are engaged in a criminal investigation? That may well count as "execut[ing] the laws";²¹⁸ the Armed Forces would be gathering information, probably at the FBI's direction, that is specifically intended to be used as evidence in subsequent criminal proceedings. Military officers thus could find themselves criminally liable under the Posse Comitatus Act because of how the FBI chooses to use the information it receives. Perversely, what would trigger liability would not be the military's own actions, but the actions of the recipient agency.

Even worse, the character of the FBI's investigation may not be readily apparent, and it may even change over time; retroactivity problems can occur here, too.²¹⁹ In the immediate aftermath of the attack, it is unlikely that the Bureau will have decided whether to put the matter on the criminal track or the intelligence track.²²⁰ It will want to keep its options open. Indeed, one of the principal aims of the early stages of the investigation will be to learn enough about the attack to decide whether it warrants treatment as a garden-variety crime or whether it is significant enough to be treated as an intelligence matter. This is the stage of the investigation when the military's assets will prove most helpful to the FBI. But it's also the stage when the investigation's character—is it criminal or is it intelligence?—is most difficult to pin down. That ambiguity encourages the Armed Forces to sit on the sidelines just when their resources are needed the most. Why take a chance and risk two years in jail? Now suppose the FBI initially decides to

215. See POSNER, *supra* note 24, at 101 (referencing the "marriage of criminal investigation and domestic intelligence in the FBI").

216. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION PRIOR TO THE SEPTEMBER 11 ATTACKS 10 (2005) [hereinafter FBI REPORT] ("International terrorism could be investigated as both an intelligence and as a criminal investigation.").

217. See JAMES P. HARVEY, NOT IN OUR OWN BACKYARD: POSSE COMITATUS AND THE CHALLENGE OF GOVERNMENT REORGANIZATION 16–17 (2008) (describing an example of the Department of Defense sharing information with the FBI after the latter launched an intelligence investigation of the 1996 Khobar Towers attack).

218. 18 U.S.C. § 1385.

219. See *supra* note 140 and accompanying text.

220. See FBI REPORT, *supra* note 216, at 19–20 (describing the different procedures and requirements for opening criminal and intelligence investigations).

treat the attack as an intelligence matter, but after receiving information from the military it changes course and opens a criminal investigation. At the time the sharing took place, it had no connection to a law enforcement investigation and thus was lawful under the Posse Comitatus Act. Now? It's hard to say. Sharing that was once lawful could become retroactively unlawful, due to the Bureau's about-face. (The Constitution's *ex post facto* clause presumably would bar the retroactive imposition of criminal liability for data exchange that was lawful at the time it took place.²²¹)

Up to this point we have only considered data flowing in one direction—from the Armed Forces to law enforcement. What about sharing in the opposite direction? Might the Posse Comitatus Act restrict the FBI from sharing data collected in the course of a criminal investigation with the military? Suppose prosecutors discover through grand jury testimony that the mall bombing was carried out by an al Qaeda cell that trained at a previously unknown camp in Yemen. May they alert the military in the hopes that the Armed Forces will raze the camp?

This sort of transaction is not covered by the 1981 amendment. That exception only authorizes sharing from soldiers to cops; it is silent on sharing from cops to soldiers. “The *Secretary of Defense* may . . . provide . . . *civilian law enforcement officials* any information collected during the normal course of military training or operations.”²²² The 1981 legislation thus may have something like an *expressio unius* effect, ruling out data exchange between the military and law enforcement that is not specifically authorized.²²³ Congress's decision to allow certain kinds of sharing implies a deliberate decision to preclude all other kinds. The question then becomes whether, in Posse Comitatus terms, the Armed Forces “execute the laws” when they use in military operations data that was gathered for law enforcement reasons. Information that originally was collected for law enforcement conceivably might retain that character even when passed on to different government officials who mean to use it for different (though related) purposes. This kind of exchange isn't obviously unlawful, but it doesn't have to be. For a government official looking at a two-year jail term, legal uncertainty may be enough to deter information sharing.²²⁴

221. U.S. CONST. art. I, § 9, cl. 4.

222. 10 U.S.C. § 371(a) (2006) (emphasis added).

223. See 2A NORMAN J. SINGER & J.D. SHAMBIE SINGER, SUTHERLAND STATUTORY CONSTRUCTION § 47:23 (7th ed. 2007). According to the Singer treatise,

As the maxim [*expressio unius est exclusio alterius* (the expression of one is the exclusion of others)] is applied to statutory interpretation, where a form of conduct, the manner of its performance and operation, and the persons and things to which it refers are designated, there is an inference that all omissions should be understood as exclusions.

Id.

224. See *supra* note 75 and accompanying text.

D. *Privacy Act*

Most commentators agree that the Privacy Act of 1974 doesn't impose meaningful limits on the ability of intelligence agencies to share information with one another.²²⁵ While the Act sweepingly bars officials from disclosing covered records without the data subject's consent,²²⁶ it is riddled with loopholes that give agencies fairly wide latitude to exchange data.²²⁷ Or so the story goes. I will argue that, in reality, the Privacy Act's exemptions are not as gaping as is commonly supposed, and the Act—especially its requirement that any “routine” disclosure of data from one agency to another must be “compatible” with the purpose for which it originally was collected²²⁸—could saddle officials with serious sharing restrictions.

At the risk of stating the obvious, the Privacy Act promotes *individual privacy*. The statute vindicates both aspects of privacy discussed above—privacy as freedom from the government observing personal facts about oneself, and privacy as the ability autonomously to control the manner in which one's information is presented to others.²²⁹ The Privacy Act—Congress's first systematic effort to protect the privacy of personal information against government intrusions—was passed because of anxiety about fast-moving technological developments.²³⁰ Computer-based systems were being deployed, both in government and in the private sector, that were capable of storing, indexing, and retrieving previously unimaginable troves of data, and Congress grew increasingly worried about the baleful consequences of these new technologies for individual privacy.²³¹

225. See Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 694–97 (2007) (arguing that the Privacy Act should be amended to better protect information privacy, including by eliminating “[f]ree-for-all information sharing”); see also Fred H. Cate, *Governing Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 465–66 (2008) (describing the numerous broad exceptions in the Privacy Act).

226. 5 U.S.C. § 552a(b) (2006).

227. Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 379.

228. 5 U.S.C. § 552a(7).

229. See *supra* notes 65–71 and accompanying text.

230. See Privacy Act of 1974, Pub. L. No. 93-579, § 2(a), 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2006)) (“[T]he increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information.”).

231. See, e.g., S. REP. NO. 93-1183, at 15 (1974) (“[T]he creation of formal or de facto national data banks, or of centralized Federal information systems without certain statutory guarantees would . . . threaten . . . the values of privacy and confidentiality in the administrative process.”); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 35 (2003) (citing “the rapid development in record-keeping systems in both government and the private sector,” as well as “the computerization of information storage, retrieval, and data processing,” as influencing Congress's decision to enact the Privacy Act).

The Privacy Act addresses that concern in a number of concrete ways.²³² Its most significant feature is its sweeping requirement that “[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.”²³³ Congress saw this nondisclosure requirement as “one of the most important, if not the most important, of the bill.”²³⁴ The Act contains a number of exceptions to its general prohibition on unconsented sharing of personal data.²³⁵ By far the most important is the exemption that allows records to be shared for a “routine use.”²³⁶ Under this provision, an agency is allowed to disclose a covered record to other officials if two hurdles are cleared. First, the “use of such record [must be] for a purpose which is compatible with the purpose for which it was collected”;²³⁷ second, the agency must publish a notice in the Federal Register.²³⁸

The conventional wisdom is that, thanks to these and other loopholes, the Act does an exceptionally poor job of protecting individual privacy. The Act has been described as “less protective of privacy than may first appear”²³⁹ and “weak and ineffectual by today’s standards.”²⁴⁰ And those are the favorable reviews. Others say the Privacy Act is either “a paper tiger,”²⁴¹ or “purely hortatory” and “entirely ineffective,”²⁴² or little more than “a procedural notice statute, rather than a safeguard against government invasion of individual privacy.”²⁴³ There is also widespread agreement that the Act doesn’t prevent intelligence agencies from swapping data. The Markle Foundation’s Task Force on National Security in the Information Age confidently predicted that “future government initiatives promoting increased interagency information sharing to protect national security will meet with little resistance” from the Privacy Act.²⁴⁴ Academic commentators

232. See, e.g., 5 U.S.C. § 552a(e)(5) (directing agencies to maintain their records accurately); *id.* § 552a(d) (guaranteeing persons the right to inspect any records pertaining to them and to correct any inaccurate information).

233. *Id.* § 552a(b).

234. H.R. REP. NO. 93-1416, at 12 (1974); see also, e.g., BeVier, *supra* note 69, at 479 (describing the nondisclosure requirement as “the heart of the Privacy Act”).

235. See *supra* note 227 and accompanying text.

236. 5 U.S.C. § 552a(b)(3).

237. *Id.* § 552a(a)(7).

238. *Id.* § 552a(e)(4)(D).

239. Cate, *supra* note 225, at 465.

240. Nehf, *supra* note 231, at 40.

241. BeVier, *supra* note 69, at 479.

242. Bignami, *supra* note 225, at 633.

243. Todd Robert Coles, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 979 (1991).

244. MARKLE FOUND., PROTECTING AMERICA’S FREEDOM IN THE INFORMATION AGE 130 (2002).

agree. "Certainly," one article intones, "this allows all agencies involved in counterterrorism to share information."²⁴⁵

The Privacy Act's exemptions may be fairly broad, but they do not give agencies anything like *carte blanche* to exchange intelligence with one another. Even the much maligned routine use exemption may prohibit a great deal of information sharing. To be sure, some courts interpret the compatibility requirement fairly weakly. But others courts regard compatibility as a significant hurdle.²⁴⁶ Routine use could prove a meaningful constraint on data exchange under this latter approach.

The most restrictive readings come from the Third and Ninth Circuits. In *Britt v. Naval Investigative Service*,²⁴⁷ the defendant agency disclosed information about a Marine Corps reservist to his employer, the Immigration and Naturalization Service (INS); Britt was the subject of a criminal investigation and the NIS believed the INS "might find it relevant to have information suggesting [his] lack of integrity."²⁴⁸ The court found the disclosure impermissible, holding that mere "[r]elevance" does not satisfy the routine use exemption's compatibility requirement.²⁴⁹ "Congress limited interagency disclosures to more restrictive circumstances," it explained.²⁵⁰ "There must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."²⁵¹ Under the Third Circuit's approach, records that one agency gathers for law enforcement purposes may not be shared with another agency even if they concededly would be relevant to the latter's mission. The Ninth Circuit took a similar tack in *Swenson v. U.S. Postal Service*.²⁵² The plaintiff, a mail carrier in California, wrote letters to a senator and congressman alleging that her postmaster was deliberately

245. Dempsey & Flint, *supra* note 70, at 1475; *see also* BeVier, *supra* note 69, at 477 (arguing that the Act "place[s] relatively few substantive barriers in the way of inter- or intra-governmental sharing of personal information"); Bignami, *supra* note 69, at 672 (arguing that agency use of intelligence information is "almost entirely unregulated" by the Act).

246. *See* MARKLE FOUND., *supra* note 244, at 129-30 (indicating that at least one court has interpreted the compatibility requirement strictly, requiring the showing of a meaningful nexus before the compatibility exception can be satisfied); Coles, *supra* note 243, at 999 ("Judicial enforcement of the . . . compatibility test[] has successfully prevented some abuses of the routine use exemption by federal agencies."); *cf.* BeVier, *supra* note 69, at 482-84 (noting that because the statute does not "prescribe a standard of compatibility," government agencies are free to interpret the provision narrowly or quite broadly and that the broad interpretations of the provision are the most worrisome); Cate, *supra* note 225, at 465 ("According to the Office of Management and Budget, 'compatibility' covers uses that are either (1) functionally equivalent or (2) necessary and proper.").

247. 886 F.2d 544 (3d Cir. 1989).

248. *Id.* at 549.

249. *Id.*

250. *Id.*

251. *Id.* at 549-50.

252. 890 F.2d 1075 (9th Cir. 1989).

undercounting rural mail routes.²⁵³ In response to inquiries from those officeholders, the Postal Service revealed that the plaintiff had filed a sex discrimination complaint with the EEOC.²⁵⁴ The court ruled that the disclosure (the purpose of which was to respond to a congressional inquiry) was not compatible with the purpose for which the information was collected (namely, “to adjudicate complaints of alleged discrimination and to evaluate the effectiveness of the EEO program”).²⁵⁵ Citing the Third Circuit’s ruling in *Britt*, the court emphasized that “compatibility requires more than mere relevance.”²⁵⁶

The D.C. Circuit takes a more flexible view of routine use. In *U.S. Postal Service v. National Association of Letter Carriers*,²⁵⁷ the court held that the compatibility requirement did not bar the Postal Service from complying with an arbitration award directing it to turn over employee information to the union.²⁵⁸ The court reasoned that, “in common usage, the word ‘compatible’ means simply ‘capable of existing together without discord or disharmony.’”²⁵⁹ It therefore concluded that disclosures are only impermissible if they would undermine the agency’s reasons for collecting

253. *Id.* at 1076.

254. *Id.*

255. *Id.* at 1078 (quoting 47 Fed. Reg. 1203 (Jan. 11, 1982)).

256. *Id.*; cf. *Covert v. Harrington*, 876 F.2d 751, 755 (9th Cir. 1989) (remarking that collection of data for security clearance purposes would not be compatible with disclosure in connection with a criminal investigation). There are some indications that Congress preferred a restrictive understanding of the compatibility requirement. See Coles, *supra* note 243, at 971, 976 (explaining that, although the House Bill’s routine use exemption reflected an incremental approach to safeguarding individual privacy in personal information, the House Committee recognized the potential for abuse and therefore “pledged to oversee vigorously federal agency use of the exemption”). The House version of the bill would have allowed agencies to disclose records pursuant to a routine use; the Senate rejected such an exemption for fear that agencies would abuse it. *Id.* at 976. The compromise was to retain the House’s routine use exemption while adding the compatibility requirement to limit agency discretion to transfer information. *Id.* at 978 (“While the House bill permitted the federal agency discretion when establishing routine uses, the compromise language required that the routine use be compatible with the purpose for which information was collected.”). Later, various members of Congress would reiterate their understanding that the compatibility requirement had some bite. See, e.g., H.R. REP. NO. 101-927, at 67 (1990). The Report notes:

Agencies proceed on the apparent belief that any disclosure can be authorized as long as a routine use has been established in accordance with the Privacy Act’s procedures. This is a distortion of the law. There must be a connection between the purpose of the disclosure and the purpose for which the information was collected. In the absence of a sufficient nexus between these two purposes, an agency cannot create routine uses simply because a disclosure would be convenient or to avoid the procedural requirements established in [the nondisclosure provision] of the Privacy Act.

Id.

257. 9 F.3d 138 (D.C. Cir. 1993).

258. *Id.* at 145–46.

259. *Id.* at 144 (quoting WEBSTER’S THIRD NEW INTERNATIONAL DICTIONARY 463 (2d ed. 1971)).

the data in the first place.²⁶⁰ “[S]o long as a proposed disclosure would not actually frustrate the purposes for which the information was gathered, [the compatibility] requirement would be met. Only in rare cases would disclosure run afoul of such a dictate.”²⁶¹ The court went on specifically to reject the Third Circuit’s reasoning in *Britt*, partly because such a restrictive understanding “would forbid an agency from disclosing information pursuant to a routine use unless its purpose in disclosure would be virtually identical to its purpose in gathering the information in the first place.”²⁶² For the D.C. Circuit, routine use isn’t much of a limit on interagency information sharing.²⁶³

Many types of information sharing would be impermissible under the Third and Ninth Circuits’ strict reading of compatibility. Consider two examples. First, U.S. Customs and Border Protection collects basic information about container ships transporting goods to the United States—e.g., the names of the crew, previous ports of call, the owners of the vessels, the owners of the cargo, and so on.²⁶⁴ The agency uses this data to identify vessels that might be carrying contraband, such as illegal narcotics or counterfeit goods that infringe various intellectual property rights.²⁶⁵

260. *Id.*

261. *Id.*

262. *Id.* at 145.

263. The Office of Management and Budget—the agency that administers the Privacy Act—apparently has cast its lot with the D.C. Circuit’s permissive approach. According to OMB, a disclosure satisfies the compatibility requirement if the recipient agency’s intended use is either “functionally equivalent” or “necessary and proper” to the sharing agency’s use. Privacy Act of 1974; Guidance on the Privacy Act Implications of “Call Detail” Programs to Manage Employees’ Use of the Government’s Telecommunications Systems, 52 Fed. Reg. 12,990, 12,993 (Apr. 20, 1987). If “necessary and proper” in the Privacy Act context means something similar to what it famously means in the Constitution, it should be fairly easy to establish compatibility. See *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316, 421 (1819) (holding that, if the end is “legitimate,” then “all means which are appropriate, which are plainly adapted to that end, [and] which are not prohibited” are “necessary and proper” within the meaning of the Constitution). Because OMB is charged by Congress with administering the Privacy Act, its interpretation of the scope of the compatibility requirement may be entitled to judicial deference under the *Chevron* doctrine. See *Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837, 844 (1984) (holding that explicit gaps in delegations of statutory authority to administrative agencies are to be construed as express delegations of authority to interpret by regulation, given controlling weight by the courts unless arbitrary, capricious, or manifestly contrary to statute).

264. See U.S. CUSTOMS AND BORDER PROTECTION, CBP FORM 1302, INWARD CARGO DECLARATION (2009), available at http://forms.cbp.gov/pdf/CBP_Form_1302.pdf (collecting previous port, vessel owner, and cargo owner information); U.S. CUSTOMS AND BORDER PROTECTION, CBP FORM I-418, PASSENGER LIST—CREW LIST (2009), available at http://forms.cbp.gov/pdf/CBP_Form_I418.pdf (collecting crew and previous port information).

265. See Press Release, U.S. Customs and Border Protection, CBP Officers Seized More Than \$5 Million in Narcotics and Currency at Laredo Port of Entry (Mar. 8, 2010), available at http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/march_2010/03082010_2.xml (providing an example of narcotics seizures resulting from Customs’s searches of shipping at a port of entry); Press Release, U.S. Customs and Border Protection, Miami CBP Seizes Counterfeit Designer Merchandise Valued at \$5.2 Million (Mar. 24, 2010), available at <http://www.cbp.gov/>

Suppose Customs wants to hand over its records to the NSA. It reasons that, if analyzing vessel data is a good way to detect contraband, it may also be a good way to detect al Qaeda operatives trying to sneak into the country. And Customs knows that the NSA's analytical capabilities are more advanced than its own. Would NSA's use of the records for counterterrorism purposes be compatible with the purposes for which Customs originally compiled them—namely, to detect knockoff Jackie Chan DVDs and Mickey Mouse dolls stuffed with heroin? A court following *Britt* might conclude that there's a fundamental difference between using data to screen for contraband and using data to screen for suspected terrorists; there's no "concrete relationship," "similarity," or "meaningful degree of convergence" between screening for goods and screening for people,²⁶⁶ the two purposes aren't "virtually identical."²⁶⁷

Second, the Environmental Protection Agency collects information about factories and other sources of air pollution, such as the names of facility owners, contact information for managers, and emissions levels. It does so to enforce the Clean Air Act—e.g., to determine whether regulated entities are emitting pollutants without the requisite permits, to assess whether a given source's emissions exceed its permitted allotment, and so on.²⁶⁸ Suppose the EPA wants to share its records with Homeland Security. DHS thinks the data will come in handy for a number of its counterterrorism responsibilities—to help assess the vulnerability of the nation's critical infrastructure to terrorist attacks, to determine the likely consequences for the surrounding areas of a terrorist attack on a plant, and to inform its decisions about which parts of the country should receive preparedness grants. Would DHS's terrorism-related use of the records be compatible with the EPA's enforcement-related reasons for collecting them in the first place? Again, the answer is far from obvious. A court may reason that there is no nexus between using factory data to limit the amount of sulfur dioxide released into the atmosphere, on the one hand, and using it to prevent terrorist attacks, on the other.

Agencies may be especially reluctant to push the information sharing envelope because of the sanctions that can be imposed for disclosing records in violation of the Privacy Act.²⁶⁹ The Act generally does not authorize penalties, criminal or otherwise, against individual officers who violate its

xp/cgov/newsroom/news_releases/archives/march_2010/03242010_2.xml (providing an example of counterfeit-good seizure resulting from Customs's searches of shipping at a port of entry).

266. *Britt v. Naval Intelligence Serv.*, 886 F.2d 544, 549–50 (3d Cir. 1989).

267. *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers*, 9 F.3d 138, 145 (D.C. Cir. 1993).

268. United States Environmental Protection Agency, Facilities and Enforcement Activities Related to the Clean Air Act Stationary Source Program (Dec. 22, 2009), <http://www.epa.gov/compliance/data/results/performance/caa/>.

269. *See, e.g.*, 5 U.S.C. § 552a(g) (2006) (allowing for civil suits against the offending agency); *id.* § 552a(i) (providing for criminal penalties against certain offending employees of government agencies).

terms.²⁷⁰ But it does allow a person injured by an unlawful disclosure to bring a civil action for money damages against the offending agency.²⁷¹ To be sure, the penalties are fairly modest. An offending agency is only on the hook for the “actual damages” sustained,²⁷² not punitive damages or any resulting emotional damages²⁷³—a far cry from the prospect of jail time under the Posse Comitatus Act.²⁷⁴ Even so, the existence of penalties, however slight, for unlawful disclosures may be enough to deter intelligence agencies from exchanging data they otherwise would have been willing to share.²⁷⁵

III. Recalibrating the Law and Policy of Information Sharing

Is it possible to expand information sharing without doing violence to pretext, firewall, republicanism, and privacy values? And is it possible to preserve those principles without unduly restricting information sharing? In general, the answer to both questions is yes. Congress had good reasons to enact the National Security Act, the Posse Comitatus Act, and the Privacy Act. But the laws are overbroad; they extend beyond the harmful conduct Congress sought to prohibit and have the potential to restrict desirable information sharing. My analysis of how to accommodate these competing concerns is informed by rational choice theory—the notion that government officials act to maximize their respective interests.²⁷⁶ Looking beyond the text of the law enables us to weigh the effects that various legal requirements

270. The Privacy Act imposes criminal sanctions in a narrow set of circumstances. An official is guilty of a misdemeanor and faces up to a \$5,000 fine if he “willfully discloses” covered material “knowing that disclosure of the specific material is so prohibited” by law. *Id.* § 552a(i)(1) (emphasis added). The Act thus only punishes officials who share information despite their personal knowledge that the law prohibits it from being disclosed. If officials are merely uncertain whether a disclosure is unlawful, the Privacy Act’s criminal penalties apparently do not apply.

271. *See id.* § 552a(g)(1) (allowing for civil suits against the offending agency); *id.* § 552a(g)(4) (specifying the monetary damages allowable in civil actions under the Privacy Act).

272. *Id.* § 552a(g)(4)(A).

273. *See Doe v. Chao*, 540 U.S. 614, 617–18 (2004) (holding that uncorroborated emotional distress is not sufficient proof of “actual damages” for the purpose of claiming recovery under the Privacy Act); *Fitzpatrick v. IRS*, 665 F.2d 327, 330 (11th Cir. 1982) (noting that the legislative history of the Privacy Act indicates a congressional intent to exclude punitive damages from “actual damages”). *But see Cooper v. Fed. Aviation Admin.*, 596 F.3d 538, 540 (9th Cir. 2010) (holding that nonpecuniary damages for humiliation, mental anguish, and emotional distress constitute “actual damages” under the Privacy Act).

274. 67 U.S.C. § 1385 (2006).

275. *See supra* note 75 and accompanying text.

276. *See, e.g.*, AMY B. ZEGART, *SPYING BLIND* 1–14 (2007) (using public choice and organizational theory principles to explain intelligence failures that culminated in 9/11); *see also* O’Connell, *supra* note 35, at 1679–80 (using public choice and organizational theory principles to explain reorganization of intelligence agencies); Sales, *supra* note 13, at 304–13 (using public choice principles to explain intelligence agencies’ reluctance to share information). *See generally* WILLIAM A. NISKANEN, JR., *BUREAUCRACY AND REPRESENTATIVE GOVERNMENT* (1971) (developing a public choice account of administrative agency action); JAMES Q. WILSON, *BUREAUCRACY* (2d ed. 2000) (same).

have on incentives within military, intelligence, and law enforcement agencies. Harnessing these incentives can help reconcile the goods of information sharing, privacy, republicanism, and the like, in ways that the blunt instrument of the law by itself cannot.

As I will argue, it is unlikely that the CIA and the FBI will collaborate on pretextual surveillance. The CIA will have strong incentives to decline requests by its bureaucratic rival to collect evidence for use in criminal proceedings because doing so would harm the CIA's own interests.²⁷⁷ Similarly, sharing probably won't raise firewall concerns under the 1947 Act or the Posse Comitatus Act;²⁷⁸ data exchange can actually vindicate firewall values by mitigating agencies' incentives to use aggressive intelligence and military techniques in inappropriate spheres.²⁷⁹ Republicanism concerns—the notion that the Armed Forces must always be subordinate to civilian authorities—don't justify sharing restrictions; the potential harms are either too unlikely to materialize or too slight.²⁸⁰ Finally, information sharing may preserve privacy values more effectively than a categorical bar on data exchange; sharing can reduce agencies' incentives to engage in duplicative rounds of privacy-eroding surveillance.²⁸¹ Congress therefore should amend the National Security Act, the Posse Comitatus Act, and the Privacy Act to clearly authorize intelligence and military officials to share counterterrorism information with one another. It isn't necessary to wipe these laws from the statute books altogether; indeed, it would be inadvisable to do so. Instead, Congress should retain each Act's core prohibitions while clarifying that these restrictions don't stand in the way of data exchange.

A. *Pretext Concerns*

Like FISA, the National Security Act of 1947—which prohibits the CIA from exercising any “police, subpoena, or law enforcement powers” or performing any “internal security functions”²⁸²—embodies pretext concerns. The Act tries to keep law enforcement officers from commissioning CIA officials (whether explicitly or, more likely, with a wink and a nudge) to collect the evidence they seek under the comparatively relaxed legal standards that apply to intelligence operations.²⁸³ Maintaining the legal limits on domestic surveillance is a worthwhile goal, but the risk that the FBI will task the CIA with pretextual surveillance seems fairly low. The CIA will have strong incentives to resist the Bureau's efforts to goad it into collecting evidence for use in criminal proceedings; Agency officials will

277. See *infra* notes 284–95 and accompanying text.

278. See *infra* subpart III(B).

279. See *infra* subpart III(B).

280. See *infra* subpart III(C).

281. See *infra* subpart III(D).

282. 50 U.S.C. § 403-4a(d)(1) (2006).

283. See *supra* notes 122–33 and accompanying text.

fear that engaging in surveillance on behalf of their rival will enhance the FBI's welfare at the expense of their own.²⁸⁴ The CIA is likely to decline the Bureau's invitations for a more immediate reason as well: such surveillance runs afoul of the 1947 Act.²⁸⁵ In short, it isn't necessary to restrict data exchange between the FBI and the CIA in an effort to prevent improper tasking, because the CIA's pursuit of its institutional interests typically will accomplish the same result.

Information sharing might allow intelligence and law enforcement agencies to collaborate in ways that enable the latter to avoid some of the legal limits on their ability to collect evidence in criminal investigations. The problem is that it can be difficult to determine the precise reasons why two agencies are swapping data with one another. A sharing arrangement between the FBI and the CIA might be completely above board; the two may be running a joint operation in which the CIA conducts surveillance overseas, the FBI conducts surveillance at home, and the resulting intercepts are exchanged throughout both agencies. Or such sharing might strike at the heart of the pretext concerns embodied in the 1947 Act; the FBI may have commissioned the CIA to act as its evidence-gathering surrogate with the latter now dutifully reporting what it has found. From the standpoint of an outside observer, it will not always be apparent whether a given sharing arrangement is innocuous or sinister. It's an evidentiary problem; data exchange that raises pretext problems will look quite similar to data exchange that is entirely innocent.

Still, an information sharing wall between the FBI and the CIA is unnecessary because the two are unlikely to collaborate on pretextual surveillance. The Agency and the Bureau have spent decades waging a fierce turf war,²⁸⁶ and the CIA won't be eager to come to the aid of its interagency rival. Part of the explanation for this intense rivalry is that CIA spies and FBI cops produce competing "goods"—the agencies represent two radically different options for how to deal with national security threats.²⁸⁷ Generally speaking, criminal investigators at the FBI will want to use the standard tools of criminal law to neutralize a given terrorist—indict him for the crimes he has committed, try him, convict him, and incarcerate (or execute) him.²⁸⁸ CIA officials will want to treat the terrorist as an intelligence asset—question him to find out if he knows about plans to strike

284. See Sales, *supra* note 13, at 282–83 (arguing that intelligence agencies hoard information to ward off competition from bureaucratic rivals).

285. See 50 U.S.C. § 403-4a(d)(1) (providing that the CIA Director “shall have no police, subpoena, or law enforcement powers or internal security functions”).

286. See generally MARK RIEBLING, WEDGE: FROM PEARL HARBOR TO 9/11 (2002) (chronicling sixty years of interagency conflict in connection with incidents that range from Watergate to the Aldrich Ames spy case).

287. See POSNER, *supra* note 1, at 29–31, 173–82.

288. *Id.* at 173.

the United States, try to turn him into a double agent who can be used to feed misinformation back to al Qaeda, and so on.²⁸⁹

This rivalry will give the CIA powerful incentives not to assist FBI criminal investigations, because doing so could benefit the Bureau's interests at the expense of its own. Even in a case where the target is an ordinary criminal—i.e., a person whose conduct is not remotely related to national security concerns—the CIA will be reluctant to collect evidence for FBI criminal purposes because that would enhance the welfare of its primary bureaucratic competitor. That is, helping the FBI to conduct a criminal investigation will bolster the Bureau's influence (its ability to persuade senior executive branch policy makers, such as the President, to accept its recommendations), as well as its autonomy (its ability to achieve its priorities without interference by outside entities).²⁹⁰ The President and the Attorney General will be marginally more likely in the future to credit the Bureau's recommendations that, say, a particular mob boss should be indicted, or that a particular terrorist should be dealt with through the criminal justice system rather than military commissions. Such topcover from senior officials also will make the FBI marginally more effective at shaving off slices of turf from rival agencies and at defending its own turf against similar encroachments.

The CIA's concerns will probably be even more acute in cases where the target is a spy or terrorist who potentially could be dealt with through either law enforcement or intelligence tools.²⁹¹ Here, the cops' preferred method of prosecuting the suspect competes directly against the spies' approach of trying to flip him. For the CIA to assist an FBI criminal investigation in these circumstances would not just increase the Bureau's absolute amount of influence and autonomy. It would increase the Bureau's relative influence and autonomy at the expense of the CIA. In effect, CIA service as an FBI surrogate would have distributive consequences; it would precipitate a wealth transfer from the Agency to the Bureau. The CIA therefore will have intensified reasons not to collect criminal evidence on the FBI's behalf in the very national security cases in which the risk of pretextual surveillance is at its apogee.

CIA officials will have strong incentives not to do the FBI's bidding for a more practical reason, too: conducting surveillance for the Bureau almost certainly would violate the statutory injunction against exercising any "police, subpoena, or law enforcement powers" or performing any "internal security functions."²⁹² The outer limits of what the National Security Act of

289. Banks, *supra* note 37, at 1151.

290. See Sales, *supra* note 13, at 282–83 (explaining that intelligence officials seek to maximize their influence and autonomy, and that such conduct can contribute to interagency rivalries).

291. See Richard B. Schmitt & Greg Miller, *FBI Reportedly Widens Intelligence Gathering*, SEATTLE TIMES, Jan. 28, 2005, available at 2005 WL 1239108 (quoting a former senior CIA official expressing concern that FBI activity in traditional CIA domains such as counterterrorism constitutes a "battle for survival" for the Agency).

292. 50 U.S.C. § 403-4a(d)(1) (2006).

1947 proscribes may be ambiguous,²⁹³ but running wiretaps for the express purpose of uncovering evidence to be used in criminal proceedings satisfies anybody's definition of "law enforcement."²⁹⁴ To be sure, the Act does not make CIA law enforcement activity a criminal offense.²⁹⁵ But a statutory violation could still be costly; it could demoralize agency employees, alienate the President and other senior officials, and encourage rival agencies to poach CIA turf.²⁹⁶ Pretextual surveillance thus involves a striking asymmetry. The benefits of such surveillance would be externalized onto the FBI, but the costs would be internalized in the CIA. The cops have everything to gain; the spies have everything to lose. In light of that asymmetry, the CIA will have good reasons to refuse requests from FBI criminal investigators to conduct pretextual surveillance on their behalf.²⁹⁷

In fact, the risk of pretext under the 1947 Act is probably much lower than the risk of pretext under FISA. The USA PATRIOT Act may have increased the opportunities for FBI intelligence officials to engage in pretextual surveillance on behalf of FBI criminal investigators,²⁹⁸ but it is less likely that CIA intelligence officials and FBI criminal investigators will so collaborate. This is so because the internal rivalry between the Bureau's cops and spies appears to be less intense than the competition that characterizes FBI-CIA relations. The FBI's intelligence officials traditionally have come from the same law enforcement background as the Bureau's criminal investigators;²⁹⁹ FBI spies therefore may be more sympathetic to FBI cops' desire to collect evidence for criminal purposes than CIA spies would be. The weaker that rivalry, the more likely it is that the Bureau's spies would be willing to run wiretaps at the behest of the Bureau's cops. In short, there may be reasons to worry that PATRIOT's dismantling of the FISA wall could lead to improper coordination between the FBI's criminal and intelligence worlds. But those reservations don't justify information sharing limits between the FBI and CIA. Even if one rejects expanded coordination under FISA, it is still possible to embrace FBI-CIA data exchange to the extent it raises weaker pretext concerns.

293. See *supra* notes 126-37 and accompanying text.

294. See, e.g., *Berger v. New York*, 388 U.S. 41, 60 (1967) (considering government assertion that wiretaps represent "a most important technique" for law enforcement).

295. See 50 U.S.C. § 403-4a(d)(1) (forbidding the CIA from engaging in "law enforcement," but not making it a crime to do so).

296. See *supra* note 75 and accompanying text.

297. In some circumstances, the CIA may calculate that the expected benefits of violating the 1947 Act exceed the expected costs. See *infra* text accompanying notes 304-24. But the CIA's benefits are unlikely to outweigh its costs when the unlawful surveillance is undertaken at the FBI's behest. See *supra* note 296 and accompanying text.

298. See *supra* text accompanying notes 105-19.

299. See POSNER, *supra* note 24, at 98-99 (discussing the mechanisms by which criminal investigators and intelligence officers are evaluated and how these performance criteria attract different personalities and talents).

B. Firewall Concerns

The National Security Act of 1947 and the Posse Comitatus Act both reflect firewall values. Each seeks to isolate various aggressive national security operations that may be justified in some contexts and prevent them from contaminating other spheres where they are (at best) unjustified and (at worst) profoundly dangerous. The 1947 Act establishes a geographic and functional firewall; the CIA may operate overseas but not at home, and it may engage in intelligence but not law enforcement.³⁰⁰ Posse Comitatus, by contrast, distinguishes solely on the basis of functions; the Army and Air Force may engage in military operations but may not enforce civil laws.³⁰¹ Though the laws draw different lines, their basic rationale is the same—to prevent the CIA and the Armed Forces from undertaking violent operations in realms where they are inappropriate.

Information sharing seems to pose little risk of producing the grave firewall harms the 1947 Act and Posse Comitatus seek to avert. Data exchange is pretty far removed from the dangers those two statutes have in mind. What we worry about is the possibility that the CIA might eavesdrop on domestic political dissidents, manipulate elections, assassinate supposedly subversive political and civic leaders, and the like, not that the Agency might swap information with Homeland Security about al Qaeda operatives flying from Amsterdam to Detroit.³⁰² Similarly, we worry about heavily armed soldiers patrolling city streets like cops on the beat and deploying overwhelming violent force against fellow citizens as though they were enemies on the battlefield, not that the military might collaborate with the FBI in trying to pinpoint the location of an al Qaeda training camp in Yemen.³⁰³ It seems possible to have fairly robust information sharing between the CIA and domestic authorities on the one hand, and between the Armed Forces and civilian authorities on the other, without raising the firewall concerns embodied in the National Security Act and the Posse Comitatus Act.

In fact, a regime of expanded information sharing has the potential to vindicate firewall values more effectively than firm rules against coordinating with the CIA and the Armed Forces. This is so because data exchange can mitigate the incentives those agencies may experience to conduct surveillance or otherwise operate in ways that violate the 1947 Act or Posse Comitatus.

Imagine an intelligence system in which information sharing does not take place. Under such a regime, intelligence agencies will only gain access to the data they collect on their own. With sharing off the table, the CIA may

300. See *supra* notes 118–21 and accompanying text.

301. See *supra* notes 154–68 and accompanying text.

302. See *supra* notes 118–21 and accompanying text.

303. See *supra* notes 154–68 and accompanying text.

face irresistible pressures to undertake domestic operations to gather information it has no other way to obtain. Suppose CIA analysts know that a group of al Qaeda operatives has entered the country; the Agency wants to listen to their phone calls and read their e-mails in the hopes of discovering whether they are about to carry out an attack. The CIA can't ask the FBI to send over the communications the Bureau has intercepted, so the Agency has no alternative but to intercept the suspects' communications on its own. The same is true of the Armed Forces (although, as we will see in a moment, perhaps to a lesser extent). Suppose the Pentagon wants to learn the location of the training camp at which the al Qaeda members received instruction so it can strike the facility. Military brass can't ask the FBI for copies of the cell's intercepted communications, so they may want to gather the needed intelligence on their own—perhaps by running their own wiretaps, perhaps by sending undercover agents to observe the cell members at the mosque where they pray or the cafés they frequent.

In both cases, agencies' inability to rely on others for the intelligence they seek will incentivize them to mount operations that strike at the heart of the firewall values embodied in the National Security Act and the Posse Comitatus Act. CIA and military officials will engage in statutorily impermissible operations when they expect that the benefits of doing so will exceed the costs.³⁰⁴ The benefits side of the ledger is fairly straightforward. Among other factors, officials will weigh the tendency of the prohibited conduct to further the Agency's mission—in the CIA's case, tracking the al Qaeda cell and discerning its intentions; in the case of the military, locating and destroying the training camp. As for costs, officials will consider the opportunity cost of the unlawful surveillance—i.e., the value of the next-best choice that's given up in favor of independent surveillance. (In this hypothetical there is no next-best choice; the absence of information sharing means there is no other way for the agencies to obtain the intelligence they seek.) Officials also will weigh the expected harms of a statutory violation—public embarrassment, loss of agency influence, loss of agency turf, individual criminal liability, and so on—discounted by the probability that those violations will be detected. Those costs can be significant. The CIA and the military will not flout the 1947 Act and Posse Comitatus anytime they perceive a slight advantage—or even a significant advantage—of doing so. In many circumstances the expected costs of conducting statutorily impermissible operations will trump their expected benefits. But not always. The number of cases in which intelligence agencies calculate that unlawful operations are welfare enhancing can't be known with any precision, but it's probably greater than zero.

304. See WILSON, *supra* note 277, at xviii (explaining that some economists and political scientists apply utility maximizing theory to explain bureaucratic behavior).

For reasons of institutional self-interest and corporate culture,³⁰⁵ the military probably has weaker incentives to engage in prohibited law enforcement activities than the CIA has to engage in prohibited internal security operations. The Armed Forces traditionally have resisted Congress's calls to play a greater role in assisting law enforcement, such as in the fight against narcotics trafficking.³⁰⁶ Military brass fear, with some justification, that the institutional cop culture of scrupulous legalism will dull soldiers' battlefield instincts, resulting in less effective combat forces.³⁰⁷ Another reason for military officials' relatively weaker incentives to collect data in violation of the law is the prospect of individual criminal liability. A CIA official who violates the 1947 Act may get his agency in hot water, and his career prospects may suffer as a result, but he doesn't face any direct criminal sanctions.³⁰⁸ A military commander who directs his subordinates to engage in law enforcement functions, by contrast, may later be charged with violating the Posse Comitatus Act, a transgression that could land him in jail for up to two years.³⁰⁹

Information sharing can mitigate agencies' incentives to undertake prohibited operations. In effect, it functions as an escape valve, dissipating the pressures national security players may face to operate in statutorily prohibited spheres. If it is possible for the CIA and the Armed Forces to obtain the information they seek from, say, the FBI, there's less need for them to try to collect the data on their own—and therefore less risk that they will run afoul of firewall principles. Data exchange thus produces a substitution effect. Because information sharing is now an option, it's more costly for Langley and the Pentagon to gather data on their own in ways that could violate the 1947 Act or Posse Comitatus. In particular, information sharing increases the opportunity cost of engaging in independent surveillance in that it supplies a next-best alternative (and often a superior alternative). By increasing agencies' costs of conducting independent surveillance, data exchange reduces (even if it does not completely eliminate) their incentives to do so. Allowing the CIA and the Armed Forces to swap data with other intelligence agencies thus has the potential to vindicate firewall values even more effectively than a categorical prohibition on interagency coordination.

305. Cf. ZEGART, *supra* note 277, at 46–56 (using principles of organizational theory to explain behavior of intelligence agencies); Gregory S. McNeal, *Organizational Culture, Professional Ethics and Guantanamo*, 42 CASE W. RES. J. INT'L L. 125, 146 (2009) (same as to Armed Forces).

306. See Felicetti & Luce, *supra* note 151, at 150 (discussing Congress's attempt, as part of the 1982 DOD Authorization Act, to increase military and civilian law enforcement cooperation in the face of a worsening national drug problem, and the Pentagon's corresponding resistance).

307. See *supra* notes 167–74 and accompanying text.

308. See 50 U.S.C. § 403-4a(d)(1) (2006) (prohibiting CIA officials from exercising “police, subpoena, or law enforcement powers” but not providing any criminal penalties for violations).

309. See 18 U.S.C. § 1385 (2006) (providing that any person who “willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both”).

C. *Republicanism Concerns*

The Posse Comitatus Act seeks to preserve republicanism values—in particular, the notion that the Armed Forces must always be firmly subordinated to civilian authorities—in two distinct ways. First, by barring soldiers from participating in law enforcement, the Act prevents the military from exercising undue influence in civilian affairs.³¹⁰ Second, Posse Comitatus helps keep the military from developing an institutional perspective on law enforcement questions, thereby preserving independent domestic policy deliberations.³¹¹ These concerns are an insufficient basis for sharing restrictions. The expected costs of information sharing involving the Armed Forces are simply too small.

First, consider the costs of civilian authorities losing control of the Armed Forces. Expected cost is equal to the magnitude of the harm in question discounted by the probability that it will materialize.³¹² Such harms would be grave indeed; they would effectively mean an end to the American experiment in representative self-government. The flaw in this argument is that it is virtually impossible to imagine the military gaining undue influence in civilian affairs, let alone forcibly taking the reins of political power. The probability of such events coming to pass is miniscule, if not zero. And the likelihood that information sharing in particular will result in these harms is tinier still.

Whether military involvement in law enforcement aggrandizes the Armed Forces at the expense of civilian authorities is ultimately an empirical matter. There is not much data available on that question. But several anecdotes from centuries past to the modern era suggest that even direct military participation in basic law enforcement functions is unlikely to result in civilian authorities losing control of the Armed Forces. An early example is the Whiskey Rebellion. In 1794, the federal government raised and fielded an army to enforce a new tax on whiskey that rebellious farmers in western Pennsylvania refused to pay.³¹³ This was no ramshackle operation; the federal force was roughly the size of the Continental Army at its peak during the Revolutionary War, and President George Washington personally commanded it in the field.³¹⁴ Yet when the crisis passed, the militias were deactivated without incident and civilian authorities suffered no enduring

310. See *supra* notes 155–68, 179 and accompanying text.

311. See *supra* notes 175–91 and accompanying text.

312. See *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947) (applying this principle to the question of negligence in tort liability).

313. Nigel Anthony Sellars, *Treasonous Tenant Farmers and Seditious Sharecroppers: The 1917 Green Corn Rebellion Trials*, 27 OKLA. CITY U. L. REV. 1097, 1104 (2002). See generally THOMAS P. SLAUGHTER, *THE WHISKEY REBELLION* (1986).

314. Sellars, *supra* note 314, at 1104–05.

loss of power.³¹⁵ Another example comes from the antebellum era. The Fugitive Slave Act of 1850 required officials to return to the South any slaves who escaped from bondage.³¹⁶ Sometimes the Army conducted the returns required by the Act.³¹⁷ Yet the Armed Forces did not thereby gain lasting independence from civilian leaders. More recently, and happily, President Eisenhower in 1957 deployed the Army's 101st Airborne Division to Little Rock, Arkansas, to ensure that African-American students were able to attend the city's public schools;³¹⁸ the Army was implementing the requirements of the Supreme Court's school-desegregation rulings.³¹⁹ Again, the Armed Forces' role in enforcing civil law didn't have any prolonged effect on the distribution of power between civilian and military officials. In short, the Armed Forces have been directed to engage in law enforcement activities repeatedly (if irregularly) over the course of American history, yet civilian authorities have not thereby ceded power to the Armed Forces. If these incidents are any indication, the slope to a military coup isn't that slippery after all.

It is even less likely that information sharing between military and law enforcement officials will result in the Armed Forces gaining independence and autonomy from civilian leadership. If the army's participation in collecting federal taxes, enforcing the terms of federal statutes, and implementing Supreme Court decisions didn't result in aggrandizement at the expense of the civilian sphere, it's hard to see how the considerably more benign swapping of data between the army and the FBI could. As argued above, information sharing can actually decrease the likelihood that the Armed Forces will engage in the sorts of core law enforcement activities that raise republican concerns.³²⁰ If the military is able to acquire the information it seeks from the FBI, it will have weaker incentives to collect on its own via independent law enforcement operations.³²¹ In short, the probability that data exchange will cause civilian authorities to lose control of the Armed Forces is fairly low, and the probability of a military coup is lower still.

What of the other threat to republicanism values the Posse Comitatus Act seeks to avert? There is some risk that participating in law enforcement

315. See ROBERT W. COAKLEY, *THE ROLE OF FEDERAL MILITARY FORCES IN DOMESTIC DISORDERS, 1789–1878*, at 64–68 (1988) (discussing Washington's use of militias to maintain order during the Whiskey Rebellion).

316. See Tkacz, *supra* note 173, at 321 (citing Act of Sept. 18, 1850, ch. 60, § 5, 9 Stat. 462, 462–63 (repealed 1864)).

317. *Id.* at 321–22.

318. KAREN ANDERSON, *LITTLE ROCK: RACE AND RESISTANCE AT CENTRAL HIGH SCHOOL 4* (2009).

319. See, e.g., *Brown v. Bd. of Educ. (Brown II)*, 349 U.S. 294, 301 (1955) (directing schools to desegregate “with all deliberate speed”).

320. See *supra* subpart II(B).

321. See *supra* notes 316–20 and accompanying text.

will cause the military to develop an institutional perspective on domestic policy questions, and that—owing to the high esteem in which the public holds the Armed Forces—voters and elected officials will extend undue deference to the military’s perspective in their policy deliberations.³²² The expected cost of this outcome is fairly low, too; the magnitude of the harm is simply too small to justify restrictions on information sharing.

This concern has to do with the quality of deliberations by voters and officeholders. The fear is not that the military will gain power at expense of civilians, but rather that civilian debate will suffer. From the standpoint of classical republicanism—an ideology that was in vogue at the time of the Founding³²³—the ideal political decision-making process involves citizens reaching conclusions based on an independent, disinterested, and rational weighing of competing conceptions of the public good.³²⁴ A corollary is that citizens must set aside extraneous considerations, such as their personal self-interest, the views of other parties, and so on. If too much weight is given to military opinion, the argument goes, that will distort the rational and independent deliberations called for by republicanism principles.³²⁵ Policy will be determined, not so much by an independent assessment that a certain course of action will advance the public good, but in part because voters are simply willing to take the military’s word for it.³²⁶ In effect, citizens might delegate some of their responsibility for making informed policy judgments to the Armed Forces.³²⁷

A lot can be said against this conception of political decision making, including wondering (as liberal theorists do) whether it is possible to conceive of a public good that is anything more than the sum of individual interests³²⁸ and questioning (as scholars of political ignorance do) whether

322. See, e.g., Richard H. Kohn, *The Erosion of Civilian Control of the Military in the United States Today*, 55 NAVAL WAR C. REV. 8, 9 (2002) (arguing that the Armed Forces have significant influence on the U.S. government’s policies).

323. See, e.g., Nathan Alexander Sales, *Classical Republicanism and the Fifth Amendment’s “Public Use” Requirement*, 49 DUKE L.J. 339, 349–50 (1999) (“During the final decades of the eighteenth century, republican theory . . . dominated the American political landscape.”).

324. See MICHAEL J. SANDEL, *DEMOCRACY’S DISCONTENT: AMERICA IN SEARCH OF A PUBLIC PHILOSOPHY* 5–6 (1996) (“According to republican political theory, however, sharing in self-rule . . . means deliberating with fellow citizens about the common good and helping to shape the destiny of the political community.”); GORDON S. WOOD, *THE CREATION OF THE AMERICAN REPUBLIC: 1776–1787*, at 55 (1969) (“By definition [republican government] had no other end than the welfare of the people: *res publica*, the public affairs, or the public good.”).

325. See Kohn, *supra* note 323, at 9 (“[T]he American military has grown in influence to the point of being able to impose its own perspective on many policies and decisions.”).

326. See *id.* at 17–19 (giving examples of how “senior military leaders have been able to use their personal leverage for a variety of purposes, sometimes because of civilian indifference, or deference, or ignorance”).

327. See *id.* at 19 (describing the interaction between the Armed Forces and the public as “a policy and decision-making process that has tilted . . . toward the military”).

328. See, e.g., Morton J. Horwitz, *Republicanism and Liberalism in American Constitutional Thought*, 29 WM. & MARY L. REV. 57, 68–69 (1987) (“The republican tradition promotes the

citizens actually engage in the deliberations assumed by republican principles.³²⁹ For our purposes, it is enough to say this: it doesn't seem any more problematic for citizens to defer to the opinions of military officials than it is for them to defer to the countless other institutions whose views they might consider when forming their own opinions.

Citizens don't deliberate in a vacuum. They are situated amid numerous organs of civil society—churches, charities, fraternal associations, and the like—and they commonly look to those institutions when forming their views on the hot-button issues of the day. Imagine a voter consulting the Catholic Church's teachings on the permissibility of capital punishment when deciding whether or not to support a legislative initiative to abolish the death penalty. The quality of public deliberations doesn't suffer from this kind of consultation. To the contrary, the existence of these institutional points of view may even enrich public debate, by exposing citizens to arguments they otherwise might not have considered. Moreover, a citizen's antecedent decision that she will defer to one organization and not to another is itself presumably the product of rational and independent deliberation that is fully consistent with republican values. When choosing whether to defer to Catholic, or Baptist, or Episcopalian teachings on capital punishment, our hypothetical voter by definition does not defer to those churches; deference comes into play only *after* the voter has decided—on her own—that a particular institution is worth listening to. And even if deference to civic institutions is thought to be undesirable in general, there is no reason to single out deference to the military as especially unwelcome. Republicanism may or may not be offended by citizens deferring to the views of their churches, of the charities to which they contribute, or of the fraternal associations to which they belong. But deference to the Armed Forces distorts the deliberative process neither more nor less than deference to these other institutions. (Again, recall that the concern here is not that the Armed Forces might acquire too much power, but rather that citizens will fail to engage in disinterested and independent deliberations.) In sum, the harms that data exchange could cause to republican values are both too remote and too small to justify sharing restrictions that segregate the military from law enforcement.

D. *Privacy Concerns*

Information sharing implicates the privacy concerns that lie at the heart of the Privacy Act—and also FISA and the National Security Act—in two

concept of an autonomous public interest, whereas the liberal ideal holds that the public interest is either simply procedural or the sum of private interests.”).

329. See, e.g., Ilya Somin, *Political Ignorance and the Counter-majoritarian Difficulty: A New Perspective on the “Central Obsession” of Constitutional Theory*, 89 IOWA L. REV. 1287, 1303–05 (2004) (outlining the requirements of voter knowledge in deliberative democracy and claiming that American citizens are largely politically ignorant).

distinct senses. First, sharing can undermine one's privacy interest in avoiding government observation of personal facts; it expands the circle of officials who are privy to one's private information.³³⁰ Second, sharing can undermine one's privacy interest in autonomously controlling the manner in which personal facts are presented to the outside world; it allows the government to use private information in ways that are far removed from the purposes for which the data originally was acquired.³³¹ Ultimately, privacy and information sharing are capable of peaceful coexistence; it is possible to achieve each without doing undue violence to the other. Information sharing generally poses less of a threat to personal privacy than surveillance does, and data exchange may preserve privacy values more effectively than sharing restrictions, by reducing agencies' incentives to engage in privacy-eroding surveillance.

I argued above that information sharing can undermine privacy interests.³³² That's true, but it is important to consider the relative magnitude of those privacy costs. Sharing is generally less harmful to privacy than surveillance is. The process of acquiring a given fact about a person via wiretap or physical search typically represents a greater affront to privacy than does the sharing of that same fact with other government officials after it has been acquired. This is so because surveillance inevitably involves the collection of extraneous and innocuous—and highly sensitive—data.³³³ When the FBI wiretaps a suspect's phone, it will not just overhear the suspect's incriminating conversations about bombmaking equipment, possible targets, sources of funding and training, and the identities of other co-conspirators. Agents also may overhear entirely innocent conversations that have no relevance to the investigation whatsoever—a conversation between the suspect and his mother in Yemen, a conversation between the suspect and a co-worker about the relative merits of the Redskins and the Cowboys, a conversation between the suspect's wife and their son's teacher about his progress in school, and so on. The process of locating individual grains of wheat that will be useful requires investigators to sift through massive amounts of chaff—sensitive and irrelevant personal facts concerning not just the suspect but other people with whom he comes into contact.³³⁴ By

330. See *supra* notes 65–67 and accompanying text.

331. See *supra* notes 68–71 and accompanying text.

332. See *supra* notes 68–71 and accompanying text.

333. Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091, 1130–31 (2009).

334. See, e.g., Rachel S. Martin, *Watch What You Type: As the FBI Records Your Keystrokes, the Fourth Amendment Develops Carpal Tunnel Syndrome*, 40 AM. CRIM. L. REV. 1271, 1289–90 (YEAR) (arguing that granting officials access to too much information can undermine personal privacy and interfere with communications protected by attorney–client privilege). But see Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 2, 26, <http://stlr.stanford.edu/pdf/walker-information-exchange.pdf> (“[I]n many cases, there’s an awful lot of wheat amidst the chaff.”).

exposing investigators to these innocent and extraneous personal facts, surveillance can place severe strain on privacy values. (This is why FISA and Title III both require investigators to adopt “minimization” procedures—i.e., procedures designed to reduce the amount of innocent content that is collected and to destroy what innocent content is gathered.³³⁵)

The sharing of information among intelligence agencies usually will not produce privacy harms of this magnitude. A smaller amount of sensitive data changes hands under the typical information sharing arrangement than is acquired during typical surveillance. In many cases, intelligence agencies do not share their raw surveillance take with one another—the innocent conversations along with the incriminating.³³⁶ What are shared are the extracts—pieces of information that an analyst has processed, reviewed, and determined may be relevant to the investigation.³³⁷ As a result, an official with whom data is shared may learn nothing about the suspect’s mother, the co-worker’s football loyalties, or the teacher’s student evaluations; those conversations have been filtered out before the data reaches him. All the recipient encounters are the portions of the overheard conversations that indicate a terrorist plot may be afoot. The personal facts that intelligence agencies share often have been distilled down to their essence. They will not be accompanied by extraneous yet sensitive facts about the suspect and his circle of associates, which ordinarily will be left on the cutting room floor. So, yes, it’s true that information sharing can undermine personal privacy. But those harms need to be understood in context. Often the privacy costs of information sharing will be smaller—perhaps much smaller—than the privacy costs of outright surveillance.

In fact, an intelligence system based on widespread information sharing has the potential to vindicate privacy values even more effectively than a categorical ban on sharing. This is so because sharing can be a substitute for surveillance. In some circumstances—namely when officials deem the costs of wiretaps or physical searches to be excessive—intelligence agencies will prefer to acquire the information they seek from an interagency partner rather than by initiating a new round of surveillance. The sharing of previously gathered information thus can obviate the need for further privacy-eroding collection.

In an intelligence system whose members are free to swap data with each other, an agency that wishes to eavesdrop on a particular suspect’s communications will have, roughly speaking, two ways of doing so. It can

335. See 50 U.S.C. § 1801(h) (2006) (describing minimization procedures for FISA surveillance); 18 U.S.C. § 2518(5) (2006) (describing minimization procedures for criminal surveillance).

336. Intelligence agencies are reluctant to share their raw take for a number of reasons, including the need to protect the sensitive sources and methods they use to collect intelligence. See LOWENTHAL, *supra* note 24, at 75-76.

337. See *id.* at 55-67 (summarizing the intelligence-production cycle).

either surveil the target on its own, or it can ask an interagency partner that previously conducted surveillance of the target to hand over some of the resulting intercepts. Imagine that officials at Homeland Security are trying to decide whether to initiate electronic surveillance of two Brooklyn-based men. DHS wants to learn whether the men represent a threat to the Indian Point nuclear power plant, which is located just a few miles up the Hudson River from New York City. Officials know that, several weeks ago, the FBI ran wiretaps on the suspects' phones and also intercepted messages that were sent to and from their e-mail accounts. Will DHS engage in a fresh round of surveillance? Or will officials ask the Bureau to send them transcripts and recordings of the relevant phone calls, copies of the relevant e-mails, and the like?

In at least some cases, DHS will go with option two. Intelligence officials will choose to acquire the information they seek through data exchange when the net benefits of sharing (benefits minus costs) exceed the net benefits of fresh surveillance.³³⁸ Surveillance can be quite costly. If DHS initiates a new round of wiretaps, it will need to devote some of its finite resources to preparing an application to the FISA Court³³⁹ (and also to helping the Justice Department's Office of Intelligence Policy and Review shepherd the application through the FISA Court's approval process³⁴⁰). DHS officials will need to install and operate the taps, they may need to translate the overheard conversations and intercepted e-mails, and they will need to pore over the raw take, analyzing it for any signs of possible terrorist activity. A round of new surveillance also has opportunity costs. Every dollar and man-hour that DHS spends surveilling the Indian Point suspects is a dollar and man-hour that can't be spent investigating other possible threats. Sometimes the costs associated with fresh surveillance will be so great that DHS officials will prefer to obtain the information they want from their partners at the FBI.³⁴¹ In other words, the high cost of fresh surveillance will

338. See O'Connell, *supra* note 34, at 1675–90 (describing the costs and benefits associated with intelligence sharing).

339. See 50 U.S.C. § 1804 (2006) (outlining the application process and requirements for an order approving electronic surveillance).

340. See 9/11 COMMISSION REPORT, *supra* note 2, at 78 (noting that the Office of Intelligence Policy and Review is responsible for reviewing and presenting all FISA applications to the FISA Court).

341. For certain agencies, the costs of domestic surveillance in particular will be quite large, thereby systematically biasing them in favor of the information sharing alternative. For example, some agencies are legally prohibited from engaging in various forms of domestic surveillance, such as the CIA under the National Security Act of 1947 and the Army and Air Force under the Posse Comitatus Act. See *supra* subparts II(B) and II(C). For these agencies, the costs of surveillance will include another consideration—the expected cost of breaking the law (i.e., the magnitude of the harm associated with a statutory violation discounted by the probability it will be detected and punished). Because of these added costs, these agencies will tend to find information sharing even more attractive than fresh surveillance.

produce a substitution effect: agency officials will switch to the lower cost alternative of information sharing.³⁴²

It isn't possible to predict a priori how often intelligence agencies will decide to forego fresh surveillance in favor of information sharing. Nor is it easy to verify after the fact how often this substitution has taken place; much of the relevant data presumably remains shielded from public view by classification requirements. Still, it seems plausible that officials will prefer to obtain the information they seek via information sharing, rather than fresh surveillance, in a not-insignificant number of instances.³⁴³

The information sharing alternative imposes relatively weaker burdens on the suspects' privacy interests (and those of the people with whom they come into contact) than would be the case if a new batch of wiretaps were the only option. The targets will only be subject to one wiretap, not two. Investigators will not expose themselves to additional hours of sensitive and innocuous conversations in the hopes of discovering some new clue. If, on the other hand, data exchange is impossible—for instance, because the governing statute makes it unlawful—officials will have no real alternative but to collect the information by initiating yet another round of surveillance. This is not to say that there are *no* privacy costs associated with information sharing; plainly there are.³⁴⁴ The point I am making is a comparative one: that data exchange does a better job, relative to fresh surveillance, of preserving individual privacy.

Up to this point the analysis has focused entirely on a single kind of privacy interest—the data subject's interest in avoiding government observation. What about the other—the data subject's interest in controlling the manner in which his personal information is used? Information sharing can pit those two interests against each other. Sharing can promote a data subject's privacy interest in avoiding government observation because it reduces intelligence officials' incentives to subject him to additional rounds of privacy-eroding surveillance.³⁴⁵ But it does so precisely by violating that data subject's separate and distinct privacy interest in keeping his personal information from being widely disseminated without his knowledge or

342. Surveillance may be costly, but sharing can be costly too. Perhaps the most important cost of sharing is the opportunity cost of foregone surveillance. To stay with our hypothetical, if Homeland Security decides to forego new wiretaps and content itself with previously collected FBI data, there is a risk that an additional round of surveillance might have uncovered new information that isn't reflected in the existing FBI intercepts. In other words, the FBI may not have collected every last piece of data that's relevant to the DHS investigation; agency investigators might overhear something incriminating that the Bureau missed. Sometimes the opportunity cost of foregone surveillance will be so great as to prove decisive, tilting the balance in favor of fresh surveillance.

343. Cf. O'Connell, *supra* note 34, at 1675–76 (reporting that the 9/11 Commission advocated greater information sharing between intelligence agencies because it would, among other things, be less costly).

344. See *supra* notes 65–71 and accompanying text.

345. See *supra* notes 339–45 and accompanying text.

consent.³⁴⁶ When the Treasury Department provides the FBI with copies of a suspected terrorist's cancelled checks, it simultaneously protects the suspect from the Bureau independently rummaging through his bank records and causes the suspect to lose even more control over the uses to which his financial data are put. The vindication of the former interest depends on the violation of the latter. It's not privacy versus security, it's privacy versus privacy.

Candidly, this tradeoff—and the inevitable violation of privacy-as-control—seems an inescapable feature of information-sharing arrangements.³⁴⁷ By definition, sharing involves the dissemination of personal data to a wide range of players, almost always without the data subject's approval, and thus necessarily places strain on his privacy interest in controlling how his information is presented to others. But that is not a decisive objection to data exchange. Given the counterterrorism benefits of information sharing, we might be willing to tolerate some reduction in our ability to determine how our personal data is used. And the autonomy costs associated with information sharing might prove bearable since data exchange not only does not violate, but actually can preserve, the privacy interest in avoiding observation. In other words, the benefits of information sharing (improved counterterrorism and the protection of observational privacy) might outweigh the costs (violations of privacy-as-autonomy).

Even if the various privacy costs associated with information sharing are thought to be excessive, it might be possible to preserve privacy without resorting to outright restrictions on data exchange. Other potential safeguards may achieve an adequate level of privacy protection—or, to say something similar, a tolerable level of privacy infringement—while ensuring that the individual mosaic tiles circulate more or less freely among the nation's counterterrorism players.³⁴⁸ For instance, the Intelligence Community might make more extensive use of anonymization tools.³⁴⁹ Data that is to be shared with interagency partners (or even within a particular

346. See Bignami, *supra* note 69, at 669 (arguing that when government agencies collect, combine, and manipulate information on individuals without their consent, they “breach” the “essential liberal duty” of respecting citizens’ choices “to keep certain matters private and to make other matters public”); Dempsey & Flint, *supra* note 70, at 1462 (explaining that, in certain contexts, “privacy is about control, fairness, and consequences, rather than simply keeping information confidential”).

347. See Nehf, *supra* note 231, at 9–16 (describing the “modern database problem” as one in which people reveal their private data in order to reap the benefits and efficiencies of information sharing).

348. See generally Walker, *supra* note 334 (discussing the appropriate balance between privacy considerations and community benefits in information exchange).

349. See, e.g., Don Clark, *Entrepreneur Offers Solution For Security-Privacy Clash*, WALL ST. J., Mar. 11, 2004, at B1 (describing an innovative information-sharing system that makes information anonymous through “one-way hashing,” a mathematical technique that turns names, addresses, or other data into strings of digits that are almost impossible to convert back to their original form).

agency) could be scrubbed of all personally identifiable information, such as names and social security numbers, before it is sent to the recipient. The recipient would analyze the cleansed data, and would only need to learn individual identities if analysis turns up indications of possible terrorist activity.³⁵⁰ Or intelligence agencies could use immutable audit trails—i.e., computerized records that detail who has gained access to a particular piece of information.³⁵¹ Audit trails can be used to discipline agency personnel who have looked at personal information without adequate reasons—e.g., those who lack the necessary security clearances, or those whose job responsibilities don't provide the requisite "need to know."³⁵² Moreover, employees' awareness that audit trails exist, and that punishment awaits, might help deter them from improperly accessing personal data.

Conclusion

One lesson that virtually everyone took from 9/11 was the need to improve information sharing among the nation's national security players. Yet nearly a decade after those devastating terrorist attacks, a number of statutory walls continue to restrict the flow of data among intelligence, military, law enforcement, and other officials. The National Security Act of 1947, the Posse Comitatus Act, and the Privacy Act admirably seek to preserve fundamental policy values—the notions that cops shouldn't evade the legal limits on their surveillance powers by commissioning spies to do their dirty work for them, that spies and soldiers should restrict their violent tradecraft to spheres where it belongs, that civilian authorities must always be firmly in control of the Armed Forces, and that the government should strive to minimize harm to individual privacy. They do so, however, at a potentially significant cost to information sharing.

Fortunately, data exchange doesn't require us to discard the underlying principles on which these statutes are based. It's possible to preserve those values while at the same time increasing the flow of data among cops, spies, and soldiers. Indeed, information sharing can actually vindicate these principles more effectively than a categorical ban on data exchange. Pretext concerns generally don't necessitate limits on sharing between the FBI and CIA, since the latter's institutional self-interest naturally will predispose it

350. See MARKLE FOUND., *supra* note 244, at 146 (asserting that it would be prudent to "design systems that maintain practical anonymity for the subjects of [background] reviews"). *But see* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. (forthcoming 2010) (manuscript at 3), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (arguing that the privacy benefits of anonymization have been "vastly overstate[d]" because "[c]lever adversaries can often reidentify or deanonymize the people hidden in an anonymized database").

351. See, e.g., MARKLE FOUND., *supra* note 50, at 8 (recommending the use of immutable audit systems to facilitate both accountability and better coordination of analytical activities).

352. See MARKLE FOUND., *supra* note 244, at 16 ("Audit technology also facilitates tracking and monitoring to improve security and to prevent inappropriate access and use.").

against running wiretaps for the former's use in criminal proceedings. Data exchange among cops, spies, and soldiers may actually promote firewall values, by reducing incentives to use unsavory national security techniques in the domestic and law enforcement arenas. Republicanism concerns don't justify building an information-sharing wall around the Armed Forces, since the resulting harms are unlikely to occur. And information sharing can vindicate data subjects' privacy interests by mitigating incentives to engage in duplicative rounds of privacy-eroding surveillance.

Congress should follow its own example—the example it set in the USA PATRIOT Act—and dismantle these walls. As long as they remain on the statute books, the need for more information sharing may be a lesson we're condemned to learn over and over again.

The Right to Privacy in Light of Presidents' Programs: What Project MINARET's Admissions Reveal about Modern Surveillance of Americans

By Lisa Graves*

This is the way the world ends. This is the way the world ends. This is the way the world ends. Not with a bang but a whimper.

—T.S. Eliot, "The Hollow Men"

Introduction

Some at this symposium suggested abandoning the concept of privacy altogether¹ while others swept it away with the wave of a hand, dismissing the rubric of rules as the "fog of law."² Outside this convening, some have long lamented the death of privacy³ and some radical theorists have argued it was never born in the first place.⁴ Still, others have refused to concede either existential ground and have fought valiantly to preserve this cherished value and what it protects.⁵ I, for one, am not ready to relinquish the idea of privacy, especially at this juncture in America's history.

* Lisa Graves is the Executive Director of the Center for Media and Democracy. Some of the analysis in this Article is the result of conversations with my colleagues in the civil liberties and national security community and elsewhere over the past few years, including policy experts and allies such as Michelle Richardson, Kate Martin, Suzanne Spaulding, Nancy Chang, Wendy Patten, Mike German, Shahid Buttar, James Dempsey, Patrice McDermott, Lynne Bradley, Kate Rhudy, and Cadence Mertz, as well as former Congressman Bob Barr, Bruce Fein, and John Dean, plus experts in litigation and strategy such as Ann Beeson, Jameel Jaffer, Melissa Goodman, Cindy Cohn, Kevin Bankston, and Lee Tien, and many others too numerous to name. I am also very appreciative of the research assistance and fine editing of Brendan Fischer, University of Wisconsin Law Class of 2011. Any mistakes, of course, remain my own. And I am grateful to Professor Bobby Chesney of The University of Texas School of Law for this invitation as well as to my colleagues at the Symposium and the students on the Texas Law Review.

1. See Benjamin Wittes, Brookings Inst., *Panel 1: National Security, Privacy, and Technology (I)*, at the TEXAS LAW REVIEW SYMPOSIUM: LAW AT THE INTERSECTION OF NATIONAL SECURITY, PRIVACY, AND TECHNOLOGY (Feb. 5, 2010), <http://www.texaslrev.com/symposium/listen> (arguing that the gathering of personal data violates some unidentified value but that value is not "privacy").

2. Kim Taipale, Executive Dir., Ctr. for Advanced Studies in Sci. and Tech. Policy, Remarks Panel 5: Accountability Mechanisms, Symposium, *supra* note 1.

3. See, e.g., A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1475–1501 (2000) (detailing pre-9/11 technologies that were destroying informational privacy).

4. See, e.g., Robert H. Bork, *Neutral Principles and Some First Amendment Problems*, 47 IND. L.J. 1, 8–9 (1971) (criticizing Justice Douglas's interpretation of a constitutional right to privacy as a value inherent in several amendments to the Constitution, in *Griswold v. Connecticut*, 381 U.S. 479 (1965)).

5. See, e.g., *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899, 901 (N.D. Ill. 2006) (describing a proposed class action brought against AT&T for its release of records to the NSA); *Plaintiffs' Opposition to the Motion of Defendant AT&T Corp. to Compel Return of Confidential Documents at 1*, *Hepting v. AT&T Corp.*, No. C-06-00672-VRW, 2006 WL 1581965 (N.D. Cal. May 17, 2006)

Instead, we must reclaim privacy and re-emphasize its status as an integral component of human freedom and dignity *in spite* of the downward spiral of the law's conception of privacy; indeed, *because* of this spiral. If we do not do so now we may never be able to reclaim it. The intersection of national security "needs" and omni-surveillance technological capacity—marketed to us by corporations as great new tools of convenience to connect with our family, friends, and colleagues but also powerfully intrusive tools in the hands of the government—is simply too dangerous to essential liberty and to genuine security to be left largely unpatrolled.⁶

In my view, the constitutional touchstone of "reasonableness" is just too malleable to protect against the real dangers of the symbiotic relationship between the government and corporations, let alone the insatiable desire of the government to know more. And these were my fears before Google was a word, let alone an empire;⁷ before most of the transactions of daily life were transmuted into traffic on the Internet; and before a handful of murderers dramatically toppled the World Trade Center and smashed into the Pentagon in 2001.

Shortly after these world-altering events emerged at the outset of the 21st century, the Administration of President George W. Bush and Vice President Richard B. Cheney claimed "plenary"⁸ power, especially in the areas of search and seizure and other acquisition activities, in the name of "national security." This was a policy arena that had been governed by the Constitution's Fourth Amendment as well as a web of law—the Foreign Intelligence Surveillance Act (FISA),⁹ executive orders, and agency rules—that had been agreed to by the political branches in the aftermath of the *last* administration that had claimed unlimited power to conduct warrantless searches of Americans' communications in the name of national security, the Nixon Presidency.¹⁰

(arguing that the interception of private communications violates the First and Fourth Amendments); As this Article goes to press, Judge Vaughn Walker issued a ruling in favor of the plaintiffs in their challenge to warrantless wiretapping in the al Haramain case. *In re Nat'l Sec. Agency Telecomms. Records Litig.*, MDL Docket No. 06-1791, 2010 WL 1244349 (N.D. Cal. Mar. 31, 2010).

6. Credit for this visualization is due Alex Joel, the Civil Liberties Protection Officer of the Office of the Director of National Intelligence, who described his official role at this intersection during the Symposium. See Alex Joel, Civil Liberties Prot. Officer, Office of the Dir. of Nat'l Intelligence, Panel 2: National Security, Privacy and Technology (II), Symposium, *supra* note 1.

7. See Google, Corporate Information, Google Milestones, <http://www.google.com/intl/en/corporate/history.html> (recording the American Dialect Society's selection of "google" as the most useful word of the year in 2002).

8. See Bob Woodward, *Cheney Upholds Power of the Presidency*, WASH. POST, Jan. 20, 2005, at A07 (describing Cheney as "especially critical of anything that would undermine the president's powers as commander in chief").

9. See Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered titles of U.S.C.).

10. See Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 158 (2008) (explaining that FISA was enacted in response to the assertion of the Executive Branch that it had the power to

The main goal of this Article is to question what an unreasonable search and a reasonable expectation of privacy mean in the national security context in the aftermath of the changes made, or urged, by the Bush Administration. Rather than explore these issues abstractly, I want to view them through a lens from the past, not simply because “what’s past is prologue,”¹¹ but because I think this will illuminate some of the crucial issues obscured in the recent debates over the Bush Administration’s warrantless wiretapping activities.

This examination is informed by viewing, in the new light of more recent information, declassified descriptions of the Signals Intelligence (SIGINT) activities during the period around the passage of FISA.¹² Specifically, this Article will examine the contemporaneous statements of the National Security Agency (NSA)—in particular, a declassified Justice Department memoranda from 1976 by Dougald McMillan (the McMillan Memo)¹³—about the controversial classified program of President Richard M. Nixon called Project MINARET.¹⁴ These admissions shed light on statements about Bush and Cheney’s more recent classified and highly controversial program that was known as the “President’s Program” (PP) until it was publicly rebranded as the “Terrorist Surveillance Program” (TSP).¹⁵

When viewed together, these and other recent public statements help clarify the legal arguments about incidentally collected information. They also underscore the need for greater public understanding and debate over

search and seize outside of the limitations of the Fourth Amendment when acting to obtain intelligence for national security purposes).

11. WILLIAM SHAKESPEARE, *THE TEMPEST* 34 (Chauncey B. Tinker ed., Yale U. Press 1918).

12. Signals intelligence involves both communications intelligence and electronics intelligence. If the information intercepted is transmitted by foreign powers it frequently needs to be decrypted, so cryptanalysis plays a significant role in SIGINT as well. See Jeffrey T. Richelson, *THE U.S. INTELLIGENCE COMMUNITY* 180 (4th ed. 1999).

13. DOUGALD D. MCMILLAN, U.S. DEP’T OF JUSTICE, *REPORT ON INQUIRY INTO CIA-RELATED ELECTRONIC SURVEILLANCE ACTIVITIES* (1976), available at <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB178/index.htm>. The memo was originally released 1982 in response to a Freedom of Information Act request by James Bamford, who has written key books on the NSA’s activities, including *THE PUZZLE PALACE* (1983) and most recently *THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA* (2008).

14. MCMILLAN, *supra* note 13, at 26.

15. The PP has also been described as including extensive “data-mining” activities and without adequate privacy protections for Americans. See Shane Harris, *Homeland Sec. and Intelligence Correspondent*, *Nat’l Journal*, Address at the Brookings Institution: The Rise of America’s Surveillance State (Mar. 11, 2010), available at http://www.brookings.edu/~media/Files/events/2010/0311_surveillance_state/20100311_surveillance_state.pdf (describing the PP). For purposes of this Article, I will use “the PP” to describe the true program in my estimation because it involves more than the surveillance of terrorists. (The Office of the Director of National Intelligence has recently claimed that the government does not engage in data-mining but instead uses a technique termed “link analysis” to mine the data it acquires, which many consider to be data-mining. See OFFICE OF THE DIR. OF NAT’L INTELLIGENCE, 2009 DATA MINING REPORT 1–2 (2010), available at <http://www.fas.org/irp/dni/datamining10.pdf> (describing a narrow definition of data-mining used by ODNI to make this claim).

abstract terms of art that are now governing the NSA's collection activity, namely "minimization rules" to "minimize" the use of information "lawfully acquired." This is especially important because we have not yet been able to obtain any alternative enforcement of the warrant requirement via litigating over the PP's expanded analysis of Americans' private communications.¹⁶

My hypothesis is that FISA has been amended to ratify the NSA setting up shop within the United States to monitor the ocean of information flowing through U.S.-based electronic communications providers and Internet service providers (ISPs) in search of foreign intelligence information. I believe that the NSA's politico-military leadership considers communications of Americans thus obtained to be "incidental" to their foreign intelligence gathering efforts and, once lawfully acquired under this schema, to be fair game for ongoing analysis to some undisclosed extent.

This accessibility exposes potentially enormous quantities of personal information about Americans—transmitted daily via various ISPs and other corporate digital platforms—to virtually eternal search and analysis by the NSA, at least in theory.¹⁷ And, right now, this program is primarily governed by secret new minimization rules written by the Executive Branch, approved by FISA Court judges handpicked by Chief Justices John Roberts and William Rehnquist, and shared in some way with some serving on congressional committees, oversight committees which I fear have been captured in some ways by the Intelligence Community they are charged with regulating.¹⁸

This Article questions the constitutionality of such collection and argues that this activity demonstrates the fundamental failure of a reasonableness test to adequately protect American's rights and interests in privacy, liberty, and security. Both security and liberty are gravely harmed by accepting the porous—almost nonexistent and nearly unenforceable—boundaries for the protection of what should be considered the inalienable rights of Americans. This Article identifies critical information missing from the public discourse, a deficiency that prevents the American people from making genuinely informed democratic judgments about how best to protect our nation—our

16. See Electronic Frontier Foundation, EFF's Case Against AT&T, <http://www.eff.org/nsa/hepting> (explaining that, in June of 2009, a judge dismissed dozens of cases brought against telecommunications companies for collaborating with the NSA to wiretap Americans' communications without warrants).

17. See Jessica LoConte, *FISA Amendments Act 2008: Protecting Americans by Monitoring International Communications—Is It Reasonable?*, 1 PACE INT'L L. REV. ONLINE COMPANION (2010), <http://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1304&context=intlaw> (relaying Senator Feingold's concerns that the FISA Amendments Act could mean millions of communications between Americans and their friends, family, and business associates overseas could be legally collected).

18. See Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 103, 92 Stat. 1783, 1788, (codified at 50 U.S.C. § 1803 (2006)) (granting the Chief Justice of the United States authority to designate judges for the FISA courts).

nation *as a whole*, not only our land and our infrastructure, but also the constitutionally secured blessings of liberty that help guarantee our freedom.

This Article begins by describing in general terms the Fourth Amendment parameters for acquisition of our information and two modern strains of judicial thought about reasonableness versus warrants for government surveillance. The Article then examines certain declassified information about Project MINARET. It will then examine key statements by the Bush Administration about the PP and its rationale. The Article concludes with some observations about what this means for the privacy of the substance and transactions of Americans' daily life and the need for greater protections for the sake of liberty, security, and our future as a free people.

I. Corporate and Government Interests and Constitutional Privacy

A. Corporate "Freedom" and Incentives to Collect Information

Even before September 11th, I feared that the Fourth Amendment's interpretation would lead to major contractions in privacy based on irresistible technological advances.¹⁹ That is because the Fourth Amendment has been construed primarily to constrain the government, not corporations.²⁰

19. The Constitution states,

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

20. *See, e.g.,* United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("This Court has . . . consistently construed this protection as proscribing only governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'"). Although I am citing this precedent, I do not wish to give credit to this decision as correctly decided but merely acknowledge that it reflects the view of a majority of the Supreme Court at that time. I believe Justice White, in his concurrence, was correct to challenge this proposition, and that Justices Brennan and Marshall, in their dissent, had the better argument on the facts of this case. Furthermore, I disagree with this line of cases as a whole because there is nothing in the plain language of the first half of the Fourth Amendment that would necessarily limit its reach to only government actors: "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . ." U.S. CONST. amend. IV. Only the second half of the Fourth Amendment refers to the rules for obtaining judicial approval for a search: "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.*

As a matter of pure interpretation of the plain English language, it would have been entirely plausible for the Court, and, more importantly, for the people, to construe the first half of the Amendment as a limitation on both private and government searches and seizures and to construe the second half as providing a particular set of rules for determining the circumstances under which a government-sanctioned search or seizure may occur or be reasonable.

My views on the weight to be accorded to the drafter's intentions, or "original intent," are too voluminous to be contained in this note, but suffice it to say I believe language matters and intent

And, generally, corporations by their nature are market-driven adopters of new technologies to maximize profit and minimize fraud or theft,²¹ and so far there has been almost no commercial downside to monitoring customers and “great” upsides to gathering information about us as consumers and then analyzing and marketing it, “commodifying” us.²² Accordingly, unless closely regulated by statute, corporations could deploy unlimited new technologies to monitor, and also charge for, activities—especially when serving as a necessary or convenient conduit for personal activities such as banking, communicating, or getting medical treatment—and thus erode our reasonable expectations of privacy without violating the Constitution, as interpreted.

My thesis was that the government could and would ride piggyback on corporate knowledge and information gathering techniques. And, my worry was that the claim would be that the American people had no constitutionally cognizable privacy interests against the government knowing what the private sector knows about them. That is, although the government could not easily get away with being the search or seizure “innovator,” it could ride the coattails of the for-profit sector, hunting and gathering on the fields of personal information accumulated by various corporations.

This is so because today’s dominant constitutional test that has emerged is not whether the government has a warrant but whether *you* have a “reasonable expectation of privacy”²³ regarding the information the government seeks. And, if you had already “shared” information about yourself with a company, how could you successfully defend against the government knowing it too? However, in my view, simply because your bank, phone company, and doctor knows information about you should not mean that the government is *entitled* to it.

In fact, the Supreme Court recognized that just because your phone conversations pass through the phone company does not mean that you have

may be in conflict, especially when one considers the narrow minds of some drafters, such as the men who amended the Civil Rights Act of 1964 to limit discrimination on the basis of sex in the hopes that the societal norm of discrimination against women would make this a poison pill to sink the bill. I would be surprised, however, if some of those who ratified the Fourth Amendment did not intend or hope it would protect against unreasonable searches and seizures, no matter whether the searchers were employed by the British Crown or the chartered East India Trading Company, although the conventional wisdom is that the Bill of Rights was intended to constrain only the federal government, not private parties. See Jack Goldsmith & Daryl Levinson, *Law for States: International Law, Constitutional Law, Public Law*, 122 HARV. L. REV. 1791, 1853 (2009) (“Many of the structural provisions of the Constitution and the Bill of Rights were designed to constrain the self-serving behavior of federal officials . . .”).

21. See, e.g., Dave Hendricks, *Palm Scans Called Next Step for IDs*, WASH. TIMES, Oct. 11, 2008, <http://www.washingtontimes.com/news/2008/oct/11/palm-scans-called-next-step-for-ids/> (discussing how U.S. hospitals are following the lead of Japanese banks in installing palm scanners to combat fraud).

22. John Edward Campbell & Matt Carlson, *Panopticon.com: Online Surveillance and the Commodification of Privacy*, 46 J. OF BROADCASTING & ELECTRONIC MEDIA 586 (2002).

23. *Katz v. United States*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

waived any privacy rights against the government listening to them.²⁴ But, the Court subsequently ruled that the telephone toll information, meaning the numbers dialed and kept as part of a phone bill, are not subject to the warrant requirement on the grounds that there is no cognizable constitutional privacy interest in numbers dialed.²⁵ The Court's view was rejected in part by Congress which passed rules governing the use of "trap and trace" devices and pen registers as well as other transactional data albeit at a lower standard.²⁶ And, recently, a federal court hand-picked by the Chief Justice of the Supreme Court has permitted Americans' conversations to be collected by the government without a warrant, based on a "reasonableness" theory.²⁷ These rulings, some incorrect in my view, are discussed below.

B. Two of the Views of the Fourth Amendment and Electronic Surveillance: Warrants Versus Reasonableness

1. Warrants to Protect Against "the Uninvited Ear."—Almost a century ago, before telephones were a widely available communication necessity, a narrow-minded majority of the Supreme Court ruled that the Fourth Amendment's protections for "persons, houses, papers, and effects" was not intended to give any protection to an American's phone calls from warrantless eavesdropping.²⁸ It was not until 1967 that the Supreme Court,

24. *See id.* at 352 ("One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

25. *Smith v. Maryland*, 442 U.S. 735, 742 (1979).

26. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1868 (codified as amended at 18 U.S.C. § 3121 (2006)) (requiring warrants for pen registers and trace and trap devices); Fromkin, *supra* note 3, at 1522 (discussing the small number of statutes that place limits on the distribution of "transactional data" including the Fair Credit Reporting Act and the Cable Communications Privacy Act).

27. *See infra* section I(B)(2).

28. *Olmstead v. United States*, 277 U.S. 438 (1928). In this pernicious decision from the prohibition era, Chief Justice William H. Taft argued that phone calls did not deserve the same protection as sealed letters under the Fourth Amendment, asserting:

The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants. By the invention of the telephone 50 years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place. The language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.

Id. at 464–65. Such arguments and similar ones have been resurrected by those attempting to rationalize warrantless government access to wireless and communications for national security purposes, along with other neo-conservative attempts to reassert the notion that the Fourth Amendment should only protect property or in essence physical searches of one's home. *See* *Shafer v. South Carolina*, 532 U.S. 36, 55 (2001) (Scalia, J., dissenting) (defining the Fourth Amendment as only protecting "persons, houses, papers, and effects" and distinguishing that from a privacy right emanating from penumbras of the Constitution); Andrei Marmor, *The Immortality of Textualism*, 38

under the leadership of Chief Justice Earl Warren, corrected this severely cramped interpretation of the Fourth Amendment that had left Americans' telephone conversations constitutionally vulnerable to warrantless surveillance by the government.²⁹ In *Katz v. United States*,³⁰ the Court ruled that the Fourth Amendment required the government to obtain a search warrant before wiretapping an American's conversations.³¹ The Court noted that "[t]he premise that property interests control the right of the Government to search and seize has been discredited" and thus physical trespass was not required for a search to count under the Fourth Amendment; "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."³²

Congress responded to the Supreme Court's *Katz* decision and *Berger v. New York*,³³ decided the same term, by creating new rules to govern the issuance of warrants for electronic surveillance in the United States in the Wiretap Act.³⁴ These new rules, however, included a statutory carve-out stating that "[n]othing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President . . . to obtain foreign intelligence information deemed essential to the security of the United States."³⁵

LOY. L.A. L. REV. 2063, 2065 (2005) (putting Scalia in a group of neo-conservative thinkers); cf. Harvery A. Silvergate & Philip G. Cormier, *Old Wine in New Bottles: Cyberspace and the Criminal Law*, B. B. J., May/June 1997, at 12–13 (noting that, traditionally, computer communications have frightened the "old order" and this partially caused the Supreme Court's slow recognition of the Fourth Amendment's reach beyond physical papers and effects).

29. See *Katz v. United States*, 389 U.S. 347, 359 (1967) (holding that the surveillance in question did not pass the scrutiny required by the Fourth Amendment).

30. *Id.*

31. *Id.* This case involved a challenge to government eavesdropping on a man making a call in a public phone booth, a device that now seems like little more than a quaint literary device to aid in the transformation of Superman. The government argued that the defendant did not deserve privacy in this public space as he could be observed entering the booth, but the Court reasoned,

[W]hat he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.

Id. at 352 (internal citations omitted). In so reasoning, the Court overruled *Olmstead's* deeply flawed analysis.

32. *Id.* at 353; see also *Silverman v. United States*, 365 U.S. 505, 511 (1961) (holding that the Fourth Amendment's warrant requirement applies to the recording of the spoken word even if overheard without any "technical trespass under the local property law").

33. *Berger v. New York*, 388 U.S. 41 (1967).

34. The Wiretap Act was passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 2510–2519, 82 Stat. 212, 212–25 (codified as amended at 18 U.S.C. §§ 2510–2522 (2006)).

35. *Id.* § 2511(3) (repealed by Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511 § 201(c), 92 Stat. 1797). Pub. L. No. 90-351, § 201(b) changed 18 U.S.C. 2511(2) to read

According to the declassified McMillan Memo (the Justice Department's 1976 internal memoranda on the MINARET program), in order to "assure that NSA's operations would not be affected by the legislation, NSA General Counsel participated in the drafting of 18 U.S.C. § 2511(3), which was incorporated" in the 1968 Act.³⁶

Secretly, after the Wiretap Act passed, the NSA General Counsel reported internally that the effect of this "presidential exception" was "to remove any doubt as to the legality of the SIGINT and COMSEC activities of the Executive Branch of the Government."³⁷

[The language] preclude[d] an interpretation that the prohibitions against wiretapping or electronic surveillance techniques in other law applies to SIGINT and COMSEC activities of the federal government. Wiretapping and electronic surveillance techniques, are, therefore, legally recognized as means for the federal government to acquire foreign intelligence information and to monitor U.S. classified communications to assess their protection against exploitation by foreign intelligence activities.³⁸

This exemption from the Wiretap Act was subsequently repealed by FISA.³⁹ The NSA's involvement in drafting the exemption is not generally known, and it was not public at the time that the Supreme Court took up a case challenging the Nixon Administration's warrantless wiretapping of Americans under a claim of national security necessity, before FISA was enacted or even envisioned.⁴⁰

[n]othing contained in this chapter, or section 605 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications by means other than electronic surveillance . . . and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire and oral communications may be conducted.

36. MCMILLAN, *supra* note 13, at 85.

37. *Id.* COMSEC, as distinct from SIGINT, refers to communications security to protect information transmitted by the Department of Defense via special equipment or encryption. See James E. Meason, *Military Intelligence and the American Citizen*, 12 HARV. J. L. & PUB. POL'Y 541, 542 n.3, 549 n.37 (1989) (defining SIGINT as the intelligence discipline focusing on interception, processing, and analysis of intercepted-signals information and COMSEC as the NSA program aimed at preventing unauthorized access, disclosure, acquisition, manipulation, modification, or loss of key government information while it is being transmitted).

38. MCMILLAN, *supra* note 13, at 85. The McMillan Memo also notes that: "NSA Counsel sought, in his initially proposed draft of U.S.C. § 2511(3), to insure that no information obtained in the exercise of such Presidential powers 'shall be received in evidence in any judicial or administrative proceeding.' This proposal was substantially diluted in the statute, as passed, and was essentially nullified by the enactment of 18 U.S.C. § 3504 on October 15, 1970." *Id.* at 85-86 (internal citations omitted).

39. Wiretap Act § 2511(3) (repealed by FISA, § 201(c)).

40. See MCMILLAN, *supra* note 13, at 85. This report was confidential from the date of its completion in 1976 until 1982 when it was released pursuant to a Freedom of Information Act request, but it has not been previously re-examined in light of the claims about the PP.

In that decision, known as the *Keith* case, President Nixon's Attorney General John Mitchell had authorized warrantless wiretaps under another exception written into § 2511(3) of the Wiretap Act: nothing in this Act shall "limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government."⁴¹ The Supreme Court unanimously ruled that this provision was unconstitutional and reaffirmed the vitality of the warrant clause, stating:

Though the Fourth Amendment speaks broadly of "unreasonable searches and seizures," the definition of "reasonableness" turns, at least in part, on the more specific commands of the warrant clause. Some have argued that "[t]he relevant test is not whether it is reasonable to procure a search warrant, but whether the search was reasonable." This view, however, overlooks the second clause of the Amendment. The warrant clause of the Fourth Amendment is not dead language.⁴²

Specifically, the Court declared that "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."⁴³ The Court added that "[t]he Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. . . . The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."⁴⁴

The Court did note that the question of foreign intelligence surveillance—the other part of the old § 2511(3) as opposed to the domestic national security surveillance—was not at issue in that case.⁴⁵ That is, there was no demonstration of collaboration between foreign powers and the Americans who were subject to warrantless wiretaps.⁴⁶ This observation—this dicta—has been relied on by some to suggest that the Court would not have required a warrant had a case involving foreign intelligence come

41. Wiretap Act § 2511(3).

42. *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 315 (1972) (quoting *United States v. Rabinowitz*, 339 U.S. 56, 66 (1950)).

43. *Id.* at 316–17.

44. *Id.* at 317 (citation omitted).

45. *Id.* at 340–41 ("It is apparent that there is nothing whatsoever in this affidavit suggesting that the surveillance was undertaken within the first branch of the § 2511(3) exception, that is, to protect against foreign attack, to gather foreign intelligence or to protect national security information.").

46. *Id.* at 309 n.8.

before it.⁴⁷ But, it is not unusual for the Court to indicate what it is *not* ruling on, which is by definition not a ruling.⁴⁸

In fact, other declassified materials from the era indicate that a key reason the Ford Administration decided to negotiate with Congress about FISA was its fear of a broad Supreme Court ruling in favor of warrants for foreign intelligence gathering that intercepts Americans' communications. This concern likely arose from *Keith's* reasoning that Americans' Fourth Amendment freedoms cannot be guaranteed if surveillance was conducted solely within the discretion of the Executive Branch. And the Ford Administration had much to fear on this point because in the six years between the Court's ruling in the *Keith* case and the passage of FISA, Congress had conducted extensive investigations into foreign intelligence surveillance practices and documented innumerable violations of Americans' rights.⁴⁹

Indeed, shortly before FISA was passed, the D.C. Circuit, sitting en banc, ruled in favor of a warrant requirement in a case involving warrantless surveillance based on a foreign intelligence rationale.⁵⁰ That case, the *Zweibon* case, has been treated by proponents of warrantless surveillance as the outlier in requiring a warrant for foreign intelligence-related surveillance that involves Americans, but that view ignores the history of the situation. The *Zweibon* case's historical context is very relevant—the decision was issued in June 1975, after Seymour Hersh's front-page *New York Times* story exposing Project MINARET's extensive government spying on Americans.⁵¹ And the decision was issued *after* the Senate had authorized a special committee led by Republican Frank Church to investigate these revelations and the CIA's other secret activities known as "the family jewels."⁵² Starting

47. See, e.g., *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980) (asserting that "[t]he needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, 'unduly frustrate' the President in carrying out his foreign affairs responsibilities.").

48. See *Hanzen Paper Co. v. Biggins*, 507 U.S. 604, 609–10 (1993) (noting that the Court was not deciding based on whether a disparate impact theory of liability is available under the ADEA); *Humphrey's Executor v. United States*, 295 U.S. 602, 627 (1935) (reasoning that dicta may be followed, but is not binding).

49. See, e.g., MCMILLAN, *supra* note 13 (compiling "findings with respect to CIA electronic surveillance activities").

50. See *Zweibon v. Mitchell*, 516 F.2d 594, 614 (D.C. Cir. 1975) (plurality opinion) (holding that a warrant must be obtained if the subject of surveillance is neither an agent of nor acting in collaboration with a foreign power).

51. See Seymour Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES, Dec. 22 1974, at 1 (reporting that the CIA has illegally been spying on American citizens for years); *Intelligence: NSA: Inside the Puzzle Palace*, TIME, Nov. 10, 1975, <http://www.time.com/time/magazine/article/0,9171,913671-1,00.html> (describing NSA's role in Project MINARET and the agency's relationship with the CIA and the FBI in the project).

52. Bill Moyers Journal, *The Church Committee and FISA* (Oct. 26, 2007), <http://www.pbs.org/moyers/journal/10262007/profile2.html>; see also, The National Security Archive, *The CIA's*

in January 1975, the Church Committee “interviewed over 800 officials, held 250 executive and 21 public hearings, probing widespread intelligence abuses by the CIA, FBI and NSA”⁵³ during the first nine months of 1975, after discovering that the secret agency called NSA even existed.

Despite *Zweibon*, opponents of a warrant requirement claim their position is supported by two other cases, *United States v. Butenko*⁵⁴ and *United States v. Brown*.⁵⁵ However, not only did these cases merely follow the dicta in *Keith*, but, more importantly, the decisions predate Seymour Hersh’s MINARET exposé and the Church Committee’s investigations demonstrating how foreign intelligence gathering had been used to violate the privacy rights of countless Americans. To rely on those cases is to ignore the historical context almost entirely. Warrant opponents also point to *United States v. Truong Dinh Hung*,⁵⁶ which, despite being issued after FISA codified a warrant requirement in foreign intelligence electronic surveillance on these shores, incoherently suggested that a warrant was not required. In any case, under the facts in *Truong* which occurred before FISA was passed, a determination of individualized probable cause was made by the Attorney General as a predicate to the electronic surveillance, not a free-floating general claim of reasonableness when gathering foreign intelligence.

Although FISA’s passage pretermitted a Supreme Court ruling on the warrant requirement, I believe the Court would likely have issued a ruling consistent with *Zweibon*. This appears especially likely because the Church Committee’s revelations demonstrated that the reasoning in *Keith*—that the Fourth Amendment could not be enforced if left solely to the Executive Branch—had been vindicated, as it were, by the Church investigation. And, because the only new member of the Court between the *Keith* case and the passage of FISA was Justice John Paul Stevens,⁵⁷ it seems unlikely that a court constituted of nearly the same panel as *Keith*, post-Church, would change course and accept a blanket foreign intelligence carve out. I think this is a much truer picture of the lay of the land in the mid- to late-1970s. But for Congress’s intervention in passing FISA to mandate warrants for both targeted and untargeted electronic surveillance of Americans on these shores, the Court would likely have reached a similar result to *Keith* for foreign intelligence gathering that affects Americans.

Family Jewels, <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB222/index.htm> (providing access and descriptions to documentation related to past transgressions by the CIA).

53. Bill Moyers Journal, *supra* note 52.

54. *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc).

55. *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973).

56. 629 F.2d 908, 916 (4th Cir. 1980).

57. See David Stout & Jeff Zeleny, *After Death of a President, Tributes Are Set for Capitol*, N.Y. TIMES, Dec. 28, 2006, at A1 (noting that Justice Stevens was nominated to the Supreme Court by President Ford in 1975).

2. *The Persistence of the "Reasonableness" Argument.*—Still, some have tried to ignore *Zweibon* and the historical momentum to insist that the reasonableness, not a warrant requirement, must be the operative standard in the foreign intelligence area.⁵⁸ Two main cases issued within the context of FISA, as opposed to *Truong*, *Brown*, and *Butenko*, have either referenced or taken this position. These decisions were made by three-judge panels hand-picked by Chief Justices Rehnquist or Roberts;⁵⁹ they included only judges appointed to the federal bench by Republican presidents;⁶⁰ and they heard oral argument only from the Executive Branch.⁶¹ It is very difficult to consider these rulings to be fair in any traditional sense of the word.

In the 2002 decision, *In re Sealed Case*,⁶² the Court of Review issued a per curiam opinion described by John Yoo⁶³ as plainly written by the judge for whom he clerked, Judge Laurence Silberman. This case was the very first appeal ever from a decision of the FISA Court and under that court's procedures only the Government had the power to appeal because it was the only party to even know how the FISA Court ruled and on what basis.⁶⁴

The USA PATRIOT Act had changed the statutory standard in 2001 to permit FISA warrants even if the primary purpose of an intelligence investigation into someone in the United States was for criminal prosecution.⁶⁵ In 2002, the Justice Department issued rules on how to handle the change in this standard from a requirement that foreign intelligence be "the purpose" of the surveillance to the new requirement that it only be "a significant purpose,"⁶⁶ meaning that prosecution could be the dominant purpose, with a foreign intelligence hook. The FISA lower court ruled against these new rules in part because of the different standards, in some regards, for probable cause under FISA versus the criminal code (which

58. See, e.g., *In re Sealed Case*, 310 F.3d 717, 741–42 (FISA Ct. Rev. 2002) (emphasizing the importance of the reasonableness standard and downplaying the importance of *Zweibon*); U.S. v. Bin Laden 126 F. Supp. 2d 264, 277, 284–85 (S.D.N.Y. 2000) (highlighting reasonableness as paramount in determining the constitutionality of foreign intelligence activity).

59. See Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 103, 92 Stat. 1783, 1788 (codified at 50 U.S.C. § 1803 (2006)) ("The Chief Justice shall publicly designate three judges. . . from the United States district courts or courts of appeals who together shall have jurisdiction to review denial of any application made under this act.").

60. Bob Egelko, *War on Terrorism: Legal Affairs; Spy Court to Review Prosecutors' Powers; Ashcroft's Appeal for Looser Rules Goes to Panel*, S.F. CHRON., Sept. 1, 2002, at A3.

61. See FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, 2452 (to be codified in scattered sections of 50 U.S.C.) ("The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order. . .") (emphasis added); *In re Sealed Case*, 310 F.3d at 717 ("Government appealed from order of the Foreign Intelligence Surveillance Court").

62. 310 F.3d at 717.

63. At the time, Yoo was working for the Office of Legal Counsel on these issues.

64. *In re Sealed Case*, 310 F.3d at 719.

65. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (codified at 8 U.S.C. § 1823 (2006)).

66. OFFICE OF THE ATT'Y GEN., GUIDELINES FOR DOMESTIC FBI OPERATIONS 16–24 (2008).

might permit an end run around traditional probable cause).⁶⁷ The FISA Court of Review took up this case at the request of the Justice Department.⁶⁸

The Bush Administration in essence had changed the FISA rules based upon Yoo's secret 2001 OLC analysis, where he asserted that the administration was free to lower the standard for intelligence collection, despite the mandate of statute. However, Yoo's analysis went beyond a simple determination of the administration's ability to bypass or alter FISA's requirements, and, under an expansive recasting of the Fourth Amendment, argued that the President did not really need to go through FISA's warrant requirements at all, and could even conduct a warrantless search as long as it was "reasonable."⁶⁹ Yoo wrote that "a warrantless search can be constitutional 'when special needs, beyond the normal need of law enforcement, make the warrant and probable-cause requirement impracticable.'"⁷⁰ (Subsequently, Yoo's analysis of the requirements of FISA and the notion of unlimited executive power with regard to the PP was considered so severely flawed that it had to be withdrawn by the Justice Department.⁷¹ The Bush White House's insistence on following his analysis of the PP's legality even after serious internal legal questions were raised about it almost provoked the resignation of the Acting Attorney General, James Comey, and others.)⁷² At the time of the one-sided oral argument to the FISA Court of Review in 2002, however, these problems were not known. And it seems likely not all of the government attorneys involved in the appeal over the Patriot Act amendments to FISA knew in 2002 that Yoo had secretly taken a Hamiltonian, king-like, view of executive power and had "authorized" activities, on behalf of OLC and the Justice Department, outside of FISA's exclusive procedures based on results-oriented rationales that minimized statutory requirements and any case law to the contrary. At least

67. See *In re Sealed Case*, 310 F.3d at 737 ("The FISA court expressed concern that unless FISA were 'construed' in the fashion that it did, the government could use a FISA order as an improper substitute for an ordinary criminal warrant under Title III.").

68. See Alison Buxton, *In re Sealed Case: Security and the Culture of Distrust*, 29 OKLA. CITY U. L. REV. 917, 922 (2004) ("The Justice Department appealed two FISA Court orders authorizing electronic surveillance on the ground that the court improperly imposed restrictions on the government's foreign-intelligence gathering procedures.").

69. See SHANE HARRIS, *THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE* 167–69 (2010) (discussing how Yoo went beyond the question posed and tried to equate warrantless wiretapping of Americans with a school district's random drug testing).

70. *Id.*

71. See OFFICE OF INSPECTOR GEN., DEP'T OF DEF. ET AL., UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 11 (2009) ("[D]eficiencies in Yoo's memorandum identified by his successors in the Office of Legal Counsel . . . later became critical to DOJ's decision to reassess the legality of the [PP].").

72. See JAMES BAMFORD, *THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA* 284–85 (2008) (indicating that James Comey and several other DOJ officials intended to resign and quoting Comey as saying, "I didn't believe that as the chief law enforcement officer in the country I could stay when they had . . . done something . . . I could find no legal basis for").

two of the men in the room at the oral argument did know the administration had concluded it was not even bound by FISA's legal requirements: John Yoo and Cheney's right-hand man, David Addington. And, at that argument, Solicitor General Ted Olson argued, among other things, that warrants were not required for foreign intelligence gathering, despite FISA's command, even though that was not germane to the issues in the case.⁷³

Judge Silberman took the lead in oral argument in this case and, according to Yoo, the opinion was written in his voice; it included dicta recasting legal history and arguing that a reasonableness test should govern this area, not warrants. At the one-sided oral argument, Judge Silberman argued that the constitutional test was reasonableness, not a warrant, and "the key to the reasonableness of any search is the exterior threat," which is not what Congress determined in FISA nor what the DC Circuit (the court to which President Reagan appointed him) had last ruled on this issue in *Zweibon* nor even how a reasonable search had been evaluated generally in other cases (with reference to one's reasonable expectations of privacy).⁷⁴ Judge Silberman practically led DOJ at the argument suggesting "[t]here are two ways to look at this. One can say this is not covered by the Constitution altogether because it's inherent executive power. The second way is to say, well, it's a reasonable search because the threat is so great even if it was constitutionally covered."⁷⁵ Remember, this was the very first decision to ever be issued by the FISA Court of Review.⁷⁶

These may seem like unusual positions for a judge to take sitting on a panel given authority to handle appeals arising from the very statute Judge Silberman was arguing for eviscerating. However, it must be noted that Judge Silberman was handpicked for this special court by Chief Justice Rehnquist, whose record demonstrated significant hostility to civil liberties. And Judge Silberman had a particularly unusual distinction—he had actually testified *against* the passage of FISA, arguing that warrants should not be

73. *Id.*

74. See *U.S. v. Belfield*, 692 F.2d 141, 145 n.15 (D.C. Cir. 1982) (noting that in a prior D.C. Circuit decision "the plurality suggested in dicta that [warrantless surveillance of Americans to gather foreign intelligence] might be unconstitutional"); Transcript of Hearing at 73, *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002) (No. 02-001) available at <http://w2.eff.org/Privacy/Surveillance/FISCR/20030128-fiscr-transcript.pdf>; see also 50 U.S.C. § 1804 (1978) (amended 2008) (requiring that a federal officer receive approval from both the Attorney General and a Foreign Intelligence Surveillance judge before he can obtain a court order authorizing foreign intelligence electronic surveillance);

75. Transcript of Hearing, *supra* note 78, at 73–74.

76. In the prior two decades the Justice Department had never appealed a case from the FISA court, and only DOJ had the statutory authority to appeal because no other parties were permitted to appear before the FISA court because it functioned like a magistrate judge issuing search warrants *in camera*. See Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 106(f), 92 Stat. 1783, 1794 (codified at 50 U.S.C. § 1806(f) (2006)) (prescribing *ex parte* and *in camera* review of materials relating to electronic surveillance); *In re Sealed Case*, 310 F.3d at 719 ("This is the first appeal from the Foreign Intelligence Surveillance Court to the Court of Review since the passage of the Foreign Intelligence Surveillance Act . . . in 1978.").

required and that the courts were not fit to adjudicate cases involving foreign intelligence.⁷⁷ To suggest that he and two other Reagan appointees got the Fourth Amendment analysis right in this case's dicta is more than I can countenance. (Judge Silberman, by the way, was subsequently awarded the Presidential Medal of Honor by President George W. Bush in 2008⁷⁸ (the judge had also been appointed by Bush to serve on the Robb Commission⁷⁹)).

The second major case⁸⁰ in which reasonableness was discussed, and the only other decision ever issued by the FISA Court of Review, arose in a challenge by an Internet service provider (ISP) to directives issued by the government pursuant to the 2008 FISA Amendments Act.⁸¹ These amendments undermined the warrant requirements for electronic surveillance on these shores that had been FISA's *raison d'être*.⁸² This case again involved a special appellate review panel made up entirely by judges put on the federal bench by Republican presidents.⁸³ This panel was not randomly chosen as is the case in other intermediate appellate bodies in the Article III federal court system;⁸⁴ this panel was handpicked by the right-wing Chief

77. See *Foreign Intelligence Electronic Surveillance: Hearings Before the Subcomm. on Legislation of the Permanent Select Comm. on Intelligence*, 95th Cong. 217 (1978) (statement of Laurence Silberman), available at <http://www.cnss.org/fisa011078.pdf> (declaring that FISA was "an enormous and fundamental mistake which the Congress and the American people would have reason to regret").

78. James Gerstenzang, *Silberman, Pace Receive Bush Awards*, L.A. TIMES, June 12, 2008, at A16.

79. See STEPHANIE SMITH, CONG. RESEARCH SERV., COMMISSION ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION: ESTABLISHMENT AND COMPOSITION 4 (2006) (naming Judge Laurence H. Silberman as co-chairperson of the commission).

80. *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (In re Directives)*, 551 F.3d 1004 (FISA Ct. Rev. 2008).

81. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (to be codified in scattered sections of 50 U.S.C.).

82. See *In re Directives*, 551 F.3d at 1006 ("Subject to certain conditions, the [amendments] allowed the government to conduct warrantless foreign intelligence surveillance on targets (including United States persons) 'reasonably believed' to be located outside the United States." (citation omitted)).

83. The special appellate review panel consisted of Chief Judge Selya and Senior Circuit Judges Arnold and Winter. Lyle Denniston, *Intelligence Wiretap Power Upheld*, SCOTUSBLOG (Jan. 15, 2009, 21:38 EST), <http://www.scotusblog.com>. Chief Judge Selya was nominated by President Ronald Reagan to the First Circuit. Federal Judicial Center, Biographical Directory of Federal Judges: Selya, Bruce Marshall, <http://www.fjc.gov/servlet/nGetInfo?jid=2140&cid=999&ctype=na&inststate=na>. Senior Circuit Judge Arnold was nominated to the Eighth Circuit by President George H.W. Bush. Federal Judicial Center, Biographical Directory of Federal Judges: Arnold, Morris Sheppard, <http://www.fjc.gov/servlet/nGetInfo?jid=60&cid=999&ctype=na&inststate=na>. Senior Circuit Judge Winter was nominated to the Second Circuit by President Ronald Reagan. Federal Judicial Center, Biographical Directory of Federal Judges: Winter, Ralph K. Jr., <http://www.fjc.gov/servlet/nGetInfo?jid=2621&cid=999&ctype=na&inststate=na>.

84. See ELIZABETH B. BAZAN, CONG. RESEARCH SERV., THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW: AN OVERVIEW 5 (2007) ("The Court of Review is composed of three judges publicly designated by the Chief Justice from the United States district courts or courts of appeals.").

Justices of the U.S. Supreme Court, John Roberts and his predecessor Rehnquist.⁸⁵ In fact, the FISA Court of Review is the only court in the history of the United States, it seems, that has been constituted entirely of judges appointed to the federal bench by a single political party, at least according to the public record, since its statutory creation in 1978 over three decades ago. That should give anyone pause.

Setting this unusual partisan distinction for a judicial body aside, the FISA Court of Review upheld a directive issued to an ISP that argued that there was no foreign intelligence exception to the warrant requirement in a challenge to new powers granted by the FISA Amendments Act (FAA).⁸⁶ The FISA Court of Review, however, bootstrapped such a requirement into its decisions in part through reliance on Judge Silberman's dicta—even though the panel acknowledged that the 2002 decision did not so rule—stating that the interpretation of the decision as implicitly recognizing such an exception was “plausible.”⁸⁷

The appellate panel then drew a parallel to the so-called special needs cases (cases from the Rehnquist Court upholding random drug testing of minors and railway workers), outside the foreign intelligence context, as demonstrating rationales for searches to be governed by reasonableness, not warrants.⁸⁸ Then, in applying a reasonableness test, the panel found that national security is of the “highest order of magnitude.”⁸⁹ It also dismissed the idea that probable cause, prior judicial review, and particularity were essential to determining whether a search is reasonable, and also discounted the individualized determination that was central in the *Truong* case.⁹⁰ Instead, the panel found that the matrix of the FAA rules—broad targeting procedures, minimization procedures, the requirement that a significant purpose of the collection be to gather foreign intelligence, internal rules relating the Executive Order 12333 and other classified information—added up to satisfying a Fourth Amendment reasonableness test as reconceived by the Court of Review.⁹¹ The panel refused to entertain a facial challenge to

85. See *supra* note 5.

86. See *In re Directives*, 551 F.3d at 1011, 1012, 1010–12 (rejecting the ISP petitioner's argument that there is no foreign intelligence warrant exception by stating “[t]hat dog will not hunt,” and holding that such an exception exists “when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States”).

87. See *id.* at 1010 (“While the *Sealed Case* court avoided an express holding that a foreign intelligence exception exists by assuming *arguendo* that whether or not the warrant requirements were met, the statute could survive on reasonableness grounds, we believe that the FISC's reading of that decision is plausible.” (citation omitted)).

88. See *id.* at 1010–11 (noting that “special needs” cases dispensed with the general warrant requirement when “the purpose behind the governmental action went beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose”).

89. *Id.* at 1012.

90. *Id.* at 1012–13.

91. *Id.* at 1013.

the FAA, rejected an “as-applied” challenge, and, behaving ostrich-like in the face of the great weight of history showing that such powers could be abused, refused to consider any possibility of bad faith.⁹²

The result in the FAA challenge demonstrates the inherent flaw in the reasonableness “test.” In the national security area, the test is weighted almost entirely in the government’s favor and constitutes deference to whatever procedures the government chooses, even if they are nothing like what would be required by a warrant. This renders them, as a practical matter, almost impossible to successfully challenge, even if in other settings the government had not assiduously asserted that the overgrown judicial fiction of “state secrets” was an impediment to an adjudication on the merits of challenges to these policies by civil liberties and privacy groups and the citizens they represent. Given the expanse of time since the *Keith* case and the right-wing revolution in Supreme Court interpretation since then, however, it is perhaps not unpredictable that such a one-sided judicial panel would issue such a far-reaching ruling and never question whether such a specially constituted panel as themselves had the constitutional authority to do so.

I do think it fair to say that the Fourth Amendment has been under legal assault for much of the period since *Keith*.⁹³ The bottom line is that Republican presidents appointed eleven Supreme Court Justices in a row (and the bulk of lower court judges),⁹⁴ and the elections that led to these appointments had all included “law and order” campaigns.⁹⁵ It was no surprise that these judicial appointees embraced the erosion of many rights.⁹⁶

What emerged from the counterrevolution on the Court over the last three decades has been a brick-by-brick curtailing of the domain of warrants primarily through limiting them to wiretaps of conversations or searches of homes and a few other situations, subject to a variety of exceptions. And, what was not covered by the warrant requirement was either written out of

92. *Id.* at 1014–15.

93. See *supra* text accompanying notes 57–59, 61–63 (summarizing cases that have narrowed the central holding of *Keith*).

94. See David A. Strauss & Cass R. Sunstein, *The Senate, the Constitution, and the Confirmation Process*, 101 YALE L.J. 1491, 1506 (1992) (noting that Republican Presidents had eleven consecutive appointments to the Supreme Court).

95. See Barry C. Feld, *The Transformation of the Juvenile Court Part II: Race and the “Crack Down” on Youth Crime*, 84 MINN. L. REV. 327, 340–50 (1999) (describing the general trend of Republicans to run law and order campaigns between the 1960s and 1980s).

96. That is, during the “curtilage” of the Warren Court—at the beginning of the Burger Court when most of the members had served on the Warren Court and had a strong commitment to enforcing the warrant requirement precedent—the nation’s highest court had responded unanimously to Nixon’s claim of a right to warrantless domestic security threats, i.e., American citizens, in spite of the requirements of the Fourth Amendment. See *generally* *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297 (1972) (indicating that no Justice of the Supreme Court agreed with the argument made by the United States in its brief on the merits that a warrant exception applied for warrantless searches conducted by the President in the investigation of domestic-security threats).

the Fourth Amendment's scope or governed by whether a majority of the Court believed the person challenging the search had a "reasonable expectation of privacy" under the Amendment or, as articulated in the second FISA Court of Review decision, whether the government's internal procedures for warrantless access to the contents of American communications were reasonable when measured against a paramount threat.

Now, with this foundation of the development or devolution of the case law, let us turn back to Project MINARET to see what light it sheds on the current issues at stake.

II. What Project MINARET's Watch-Listing of Americans Reveals About Past (and Present) Analysis of "Incidentally" Intercepted Conversations

As noted above, in December 1974, the *New York Times* published a front-page story by Seymour Hersh with the headline "Huge C.I.A. Operation Reported in U.S. Against Anti-War Forces," alleging that the Nixon Administration had been engaged in a program to spy on Americans' communications, shocking Congress and the American people.⁹⁷ Three decades and a year later almost to the day, the *New York Times* published a similar story, "Bush Lets U.S. Spy on Callers Without Courts," alleging that the Bush Administration was spying on American communications despite the legal reforms and warrant requirements Congress had passed in FISA.⁹⁸ These reforms had been relied upon by the American people, in the wake of surveillance activities revealed by Hersh and the Church Committee. But, the parallels do not begin or end with the headlines.

There were also calls for criminal prosecution of CIA officers as a result of their involvement in spying on Americans' communications and other excesses under the guise of national security or foreign policy needs.⁹⁹ Similarly, many voices have called for criminal investigations, with subpoena power, to examine key decisions made within the Bush Administration regarding not just surveillance activities affecting Americans but also the torture of foreign suspects, among other highly controversial activities.¹⁰⁰

And, in another parallel, the Justice Department officials in the succeeding administrations—those of President Gerald Ford and President Barack Obama—declined prosecution.¹⁰¹ But, as interesting and troubling as

97. Hersh, *supra* note 53, at 1.

98. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

99. See *Dems Push for Look into Bush-era Policies*, CHARLESTON GAZETTE, July 13, 2009, at A2 (stating that some Democrats were pushing for investigations into programs launched by the Bush Administration).

100. See *id.* (reporting "that Attorney General Eric Holder was contemplating opening a criminal investigation into CIA torture").

101. See MCMILLAN, *supra* note 13, at 171 (declining prosecution during the Ford Administration); Steven Thomma & Marisa Taylor, *Obama Reverses Stand on Prosecution in*

these parallels are, I think the more surprising element is what a close examination of the declassified Ford-era memo reveals about past surveillance and what that means for the present, particularly because it contains little-noticed descriptions of the technology of surveillance that bear on the most recent debates about Americans' communications and privacy.

A. The Danger to Privacy and Liberty of Dividing the World of Communications in Two, Within and Without the United States

Twenty-four years ago, Dougald McMillan wrote a secret Justice Department report declining to prosecute officers at the CIA for their role in the electronic surveillance of Americans' international communications as part of President Richard M. Nixon's Project MINARET that Hersh had revealed.¹⁰² That program involved a presidential directive to the NSA to use watch lists to search through the pool of information it was collecting as part of its SIGINT operations,¹⁰³ which were focused on international communications that were plucked from the sky via radio signals and receivers as well as communications that were gathered via Operation SHAMROCK's program of acquiring almost all international telegrams into or out of the United States and analyzing them.¹⁰⁴

As detailed below, the NSA had divided the world in two in terms of electronic communications, which basically distinguished between communications with at least one foreign terminal and communications that did not have at least one end outside the United States.¹⁰⁵ This simple but false duality had the effect of treating Americans' personal international communications the same as purely foreign international communications that were not between Americans, at least at the point of acquisition and ostensibly for the purpose of analysis.

I think the better legal analysis would have been three categories of communications: Americans' domestic communications, Americans' international communications, and communications not involving Americans. This could have been reduced to a dualism: communications initiated or intended to be received by a person in the United States and all other communications as a legal matter, setting aside the technology.

Since that time, the NSA and its lobbyists and proxies have made a dramatic shift, based in part on the rise of the Internet and based in part on desire, that the world should no longer be divided in two (domestic and not

Terror Investigations, KAN. CITY STAR, Apr. 22, 2009, at A1 ("Obama repeated his stand that CIA officers should be immune from criminal charges for their work interrogating suspects . . .").

102. MCMILLAN, *supra* note 13, at 171.

103. *See id.* at 26–28 (describing Project MINARET and the NSA watch lists).

104. *See id.* at 33–34 (describing Operation SHAMROCK).

105. *See id.* at 26–27 (discussing the types of communications monitored under Project MINARET).

purely domestic), at least at the point of acquisition.¹⁰⁶ And, part of their claim was also grounded in the implicit argument that once the congressional investigations ended and the dust settled in 1978, the NSA went back to its business of using its big ears to acquire and analyze the international communications of Americans via satellites that received radio signals.

In the aftermath of the 2005 *New York Times* story, the Administration floated a bunch of legal rationales and policy arguments for the PP.¹⁰⁷ It then decided to play offense and argue in essence that what had been done was always permitted, or at least *intended* to be permitted. It also argued that the advent of the Internet, with its reliance on digital communications (optical/light rather than radio wave), had rendered the agency nearly deaf and so the law needed to be “modernized” to fix that.¹⁰⁸

The first argument is difficult to square, however, with the idea that something did change in the acquisition and analysis policies that did result in President Bush issuing new “directives” to the NSA related to Americans. These directives pertained not just to the claim if al Qaeda calls you, we want to know why. They also applied to some aspects affecting Americans’ communications that were so new and worrisome, and on such flimsy legal footing, that the acting Attorney General and the Director of the Federal Bureau of Investigation in the Bush Administration almost resigned when the Bush Administration attempted to proceed over new Justice Department objections.¹⁰⁹

It is also quite apparent from looking at the scope of the FISA Amendments Act that, as a statutory matter, the scope of the new surveillance authority is about much more than al Qaeda and gives the NSA much more authority than it had under what Ben Powell, General Counsel to the Director of National Intelligence, dubbed “classic FISA.”¹¹⁰ And, I

106. See, e.g., Charlie Savage & James Risen, *Bush-era Wiretapping Program Is Ruled Illegal; Judge Rejects ‘State Secrets’ Argument*, BOSTON GLOBE, Apr. 1, 2010, http://www.boston.com/news/nation/washington/articles/2010/04/01/bush_era_wiretapping_program_is_ruled_illegal (explaining that the NSA defended its surveillance of domestic communications on the grounds that the President’s powers permit overriding FISA).

107. See Risen & Lichtblau, *supra* note 103 (recounting some of President Bush’s constitutional, legislative, and policy rationales for the PP).

108. See *id.* (“[T]he existing Foreign Intelligence Surveillance Act was not written for an age of modern terrorism.”).

109. See Joel K. Goldstein, *The Contemporary Presidency: Cheney, Vice Presidential Power and the War on Terror*, 40 PRESIDENTIAL STUD. Q. 102, 118 (2010) (detailing meetings with James Comey, acting Attorney General, and Robert Mueller, FBI director, after learning of massive potential resignations from the Justice Department).

110. See, e.g., *Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security: Washington, Hearing on H.R. 3845 Before the S. Comm. on the Judiciary*, 111th Cong. (2009) (statement of Lisa Graves, Executive Director, Center for Media and Democracy) (noting that, while under classic FISA, the government had to identify the device to be tapped, under the 2008 amendments, the government is not required to disclose to the court the “facility” where the acquisition of electronic information takes place, let alone particular phones or internet accounts, for surveillance that meets the Act’s test).

believe it gives the NSA a scale of access, or potential access, to American communications that absolutely dwarfs what was available for analysis under Project MINARET, especially with the advent of the Internet. Accordingly, I believe we need much better protections for the freedoms of individual Americans now that the world of communication at the point of acquisition is no longer divided in two. Let us test this hypothesis.

1. The Two Realms of Electronic Communications Under MINARET.—The top secret McMillan Memo, which was subsequently declassified, has never been thoroughly (at least publicly) analyzed as part of an assessment of the claims made in the recent scandal involving a presidential directive to the NSA to search through pools of information it was previously acquiring or newly acquiring with the assistance of telecom providers following 9/11. But that memo, taken at face value, illuminates recent claims about the NSA's activities, technology, and mission vis-à-vis Americans.

a. Purely Domestic Communications of Americans.—During that Justice Department inquiry into whether CIA agents should be prosecuted for their involvement in the warrantless acquisition of American communications, the NSA itself described the two realms of communications from its vantage point. One part was the domestic communications network, which the NSA described as “contiguous, switched (from wire to cable to microwave) automatic and self-routing. Its wireless component [was a multi-channel microwave carrier system capable of carrying up to 2,000 communications on some channels.]”¹¹¹ From a layperson's standpoint, what that means is that calls within the United States between people in the United States involved both wired communications (the telephone lines into our homes and businesses, and the cables strung by the side of the road) as well as wireless communications (the beaming of communications from one part of a state to another or across the country, which was accomplished by radio wave relays). To put it more simply, most local calls were transmitted via wires and most long distance or toll calls were transmitted at least in part via radio waves.

It may come as a surprise to some that wireless domestic communications were available in the now ancient seeming technology of the 1970s,¹¹² even though personal wireless phones did not take off until the late 1980s or become a practical necessity until the first decade of the 21st century.¹¹³ However, after the Supreme Court's decision in the *Katz* case, Americans believed the Constitution required a warrant to tap into their

111. MCMILLAN, *supra* note 13, at 131.

112. ANDREA GOLDSMITH, WIRELESS COMMUNICATIONS 2 (2005).

113. *See id.* at 3 (describing the rapid development of wireless communications in the 1980s and 1990s due to advances in the technology of cellular systems).

phones, regardless of whether some part of their call traveled via wire or radio signals.¹¹⁴

Indeed, to the ordinary person, the technology used for communicating is largely separate from their liberty and privacy interests in the communication itself. Regardless of whether they use a cell phone, landline, Skype, Instant Messaging, or e-mail, regular Americans assume that their communications with their friends, family, lovers, or colleagues are private—whether the communication is across town, the state, the nation, or the globe—and believe their government would not capture or analyze their communications unless a judge ordered such surveillance based on them doing something wrong.¹¹⁵ Some may dispute whether such an expectation of privacy is reasonable, because radio signals and Internet communications may be receivable, but the question is not properly understood to be whether the government *could* intercept Americans' communications, but whether it *would* intercept them without a warrant predicated on probable cause of suspected wrongdoing. The question, at its heart, is about the relationship between the government and the governed or, more properly, between the sovereign people and the government that represents them.

In the McMillan Memo, the NSA described its discretionary decision to follow the “one-terminal rule” meaning that it voluntarily focused on communications in which at least one terminal to, or at the end of, the communications was outside the United States.¹¹⁶ That is, it had the capacity to capture all radio communications, including purely domestic communications, but it chose not to use some of this capacity based on its decision to adopt the one-terminal rule. This rule relates to its conception of international communications, as discussed below.

b. “International” Communications, Purely Foreign or Not.—The second realm, according to the NSA’s description in the McMillan Memo, was the “*international* commercial radio telephone communications [to be] transmitted by high-frequency, single or multi-channel telephony which enters the national communications network through what are known as

114. See *Katz v. United States*, 369 U.S. 347, 353 (1967) (holding that the Fourth Amendment protection from unreasonable search and seizure protects Americans in telephone booths from warrantless wiretaps); see also Deirdre Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1578 (2004) (arguing that the holding in *Smith v. Maryland*, 442 U.S. 735 (1979), that individuals do not have a reasonable expectation that the phone numbers they dial are private, is an example of the Supreme Court eroding the “reasonable expectation” prong of *Katz* in subsequent decisions).

115. See Paul Ham, *Warrantless Search and Seizure of E-mail and Methods of Panoptical Prophylaxis*, 2008 B.C. INTELL. PROP. & TECH. F. 90801, http://bciprf.org/index2.php?option=com_content&do_pdf=1&id=42 (noting that the *Katz* opinion seems to extend protection to the privacy interests of individuals, as opposed to a particular space or the penetrability of that space).

116. MCMILLAN, *supra* note 13, at 81.

‘gateways.’”¹¹⁷ The NSA described these high-frequency radio signals as easily interceptable by, for example, ship-to-shore radios or satellite.¹¹⁸ According to the NSA, such multi-channel transmission could be intercepted with radio receivers and “de-channelled,” unless they were encoded by “ciphony equipment” to garble the communications; however, none of the commercial communications carriers used that technology even though some governments did.¹¹⁹ This description certainly accounts for the NSA’s use of satellites and parabolic receivers to intercept these signals and de-channel them to focus on particular channels, such as those used during the Cold War by the Soviet Union. Under this rubric, Americans’ international communications were just as vulnerable to acquisition as purely foreign communications involving foreign nationals abroad who do not have the same constitutional rights and interests vis-à-vis the U.S. government.

Nevertheless, this picture is incomplete in a variety of ways. Such a depiction does not account for the fact that many international communications did not travel via high-frequency radio.¹²⁰ For example, international telegrams, which straddled the historical space between mailed letters in sealed envelopes and e-mail, were called cables because they were transmitted via wire, not via high-frequency radio.¹²¹

As the Church Committee revealed, however, the NSA had been acquiring and analyzing virtually all international telegrams to or from American residents and businesses for decades under the secret Operation SHAMROCK program.¹²² Moreover, the description did not take into account that the telephone companies relied on transatlantic and transpacific cables to transmit significant portions of Americans’ international calls to Europe and Asia (although communications to South America relied more heavily on radio signals, transmitted via AT&T’s satellites).¹²³ Communications within the contiguous land of Europe and Asia, however, were much more similar to that of the domestic United States, with some

117. *Id.* at 131.

118. *Id.*

119. *Id.*

120. See A SHORT HISTORY OF SUBMARINE CABLES, http://www.iscpc.org/information/History_of_Cables.htm (noting the weaknesses of high-frequency radio in transmitting internationally, including a limited capacity and the potential for atmospheric disruptions).

121. See Donald Murray, *How Cables Unite the World*, in 4 THE WORLD’S WORK: A HISTORY OF OUR TIME, MAY TO OCTOBER 2298, 2299 (Walter Hines Page & Arthur Wilson Page eds., 1902) (describing the development of a worldwide network of 200,000 miles of submarine cables for the transmission of international telegrams).

122. MCMILLAN, *supra* note 13, at 33.

123. See A SHORT HISTORY, *supra* note 126 (describing the burst in demand that followed the 1963 completion of COMPAC, a network of cables that spanned the Atlantic and Pacific Oceans and provided 80 two-way voice circuits).

communications travelling via wire and some via radio waves, making some of them easily accessible to being captured and de-channelled by the NSA.¹²⁴

2. *Using the Pool of International Communications Incidentally Collected.*—The McMillan Memo makes clear that Project MINARET sought to exploit the NSA's technological capacity to obtain information about Americans via analyzing their international communications.¹²⁵ According to the NSA, "The primary sources [of the information pool] were: (1) the NSA's interception of international commercial carrier (ILC) voice and non-voice communications [clause redacted]¹²⁶ and (2) copies or tapes of international messages furnished to NSA by U.S. commercial communications carriers in the Shamrock operation."¹²⁷

Elsewhere in the McMillan Memo the pool of communications was described as derived exclusively from these two means of interception: "all MINARET communications apparently had at least one terminal in a foreign country and, excluding SHAMROCK communications, were obtained through the interception of *radio portions* of international communications from sites both within and without the United States."¹²⁸ To be clear, this description does not mean that the NSA could access all international communications of Americans, but that all communications that were accessed had been obtained in one of these two ways.

3. *How that Pool Was Used by President Nixon.*—Just six months after taking office, President Nixon directed the NSA to use this pool to search for information on specific Americans, whom he and his allies in the Executive Branch had placed on a watch list.¹²⁹ So there can be no ambiguity, here is the precise way the NSA described the scope of the project:

MINARET (C) is established for the purpose of providing more restrictive control and security of sensitive information derived from communication as processed [redacted] which contain (a) information

124. See, e.g., MCMILLAN, *supra* note 13, at 130–31 (describing how phone calls were transmitted circa the creation of FISA).

125. See *id.* at 26 (including "U.S. organizations or individuals engaged in activities which might result in civil disturbances or otherwise subvert the national security" and "[m]ilitary deserters involved in the anti-war movement" in a list of MINARET's targets).

126. Elsewhere in the report this redacted clause is not redacted and is stated as "telex" which was basically a telegram that was transmitted not by wire or radio but by non-aural electronic pulses. See *id.* at 160 ("MINARET intelligence . . . was obtained *incidentally* in the course of NSA's interception of aural and non-aural (e.g., telex) international communications, and the receipt of GCHQ-acquired telex and ILC cable traffic . . .").

127. *Id.* at 26.

128. *Id.* at 160–61.

129. See Robert Bloom & William J. Dunn, *The Constitutional Infirmary of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment*, 15 WM. & MARY BILL RTS. J. 147, 157 (2006) (noting that from its official inception in 1969, Project Minaret was constitutionally flawed, as it constituted a *de facto* "watch list" containing the names of as many as 1,600 American citizens, and up to 800 at a given time).

on foreign governments, organizations or individuals who are attempting to influence, coordinate or control U.S. organizations or individuals who may foment civil disturbances or otherwise undermine the national security of the U.S. (b) *information on U.S. organizations or individuals who are engaged in activities which may result in civil disturbances* or otherwise subvert the national security of the U.S. An equally important aspect of MINARET will be to restrict the knowledge that such information is being collected and processed by the National Security Agency. *MINARET specifically includes communications concerning individuals or organizations involved in civil disturbances, anti-war movements/demonstrations and military deserters involved in anti-war movements.*¹³⁰

Congress discovered that, as a consequence of this directive, the NSA had about 1,200 American names, mostly persons opposing the Vietnam War, on watch lists provided by other agencies,¹³¹ such as the Bureau, which was then led by FBI Director J. Edgar Hoover.¹³² In its official findings, Congress noted that, for example, communications mentioning the wife of a U.S. Senator had been intercepted and disseminated by the NSA, as were conversations about a concert for peace, a journalist's report from Southeast Asia to his magazine in New York, and even a *pro-war* activist's invitations to speakers at a rally.¹³³

But, Project MINARET's focus was later expanded by President Nixon and his men.¹³⁴ By the beginning of 1971, it was described in an official memorandum between the Department of Defense and the Department of Justice—the scope of the NSA's searching was to obtain “[i]ntelligence bearing on: (1) Criminal activity, including drugs. (2) Foreign Support or foreign basing of subversive activity. (3) Presidential and related protection.”¹³⁵ The most significant aspect of this expansion was in the area of analyzing communications between the United States and South America for information relating to President Nixon's war on drugs and drug abuse.¹³⁶

130. MCMILLAN, *supra* note 13, at 26.

131. S. REP. NO. 94-755, at 746 (1976).

132. *Id.*

133. *Id.* at 750.

134. MCMILLAN, *supra* note 13, at 26–27.

135. Memorandum to the Secretary of Defense, the Attorney General from Vice Admiral Noel Gayler, Director, National Security Agency (Jan. 26, 1971), *reprinted in Intelligence Activities: Hearings on S. Res. 21 Before the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. (1976). For a synthesis of these and other key documents obtained by the non-profit group, the National Security Archive, from the Ford Administration's archives, see *Electronic Surveillance: From the Cold War to Al-Qaeda*, National Security Archive, <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB178/index.htm>.

136. See MCMILLAN, *supra* note 13, at 112 (“The President is intensely interested in using every means at his disposal to stop the international narcotics traffic. This includes covert action where appropriate.”). The Nixon Administration had “declared that international narcotics control was a major goal of U.S. foreign policy” thus establishing their nexus for these activities. *Id.* The CIA noted that the White House had specifically tasked G. Gordon Liddy to assist with these efforts

This nearly three-year aspect of the project involved “the interception of high-frequency radio-telephone (commercially) voice communications between the United States and several South American cities.”¹³⁷ The Church Committee found that almost 500 Americans were focused on as part of the drug interdiction elements of this surveillance.¹³⁸

4. *Rationalizing the Analysis of Americans' Private Calls.*—In 1972, the Supreme Court issued its landmark decision in the *Keith* case, holding that “Fourth Amendment freedoms cannot properly be guaranteed if domestic surveillances may be conducted solely within the discretion of the Executive Branch.”¹³⁹ But despite this declaration, Project MINARET’s analysis of its pool of communications for information about Americans did not cease. Even though President Nixon had directed the NSA to focus on Americans protesting the war in Vietnam, the Nixon Administration did not order the NSA to cease collecting or analyzing intelligence on Americans’ domestic activities in light of this Supreme Court decision. Instead, it asked the NSA to stop *disseminating* the information it was analyzing to *other* agencies.

The NSA responded to even this limited request by asserting that the collection and analysis was legitimate, despite the Supreme Court’s ruling in *Keith*. Specifically, the Director of the NSA, General Lew Allen, Jr., told President Nixon’s Attorney General Elliot Richardson that it did not collect domestic intelligence per se but that such information about Americans was simply the “by-product” of its other communications collection activities. He added:

No communications intercept activities have been conducted by NSA, and no cryptologic resources have been expended *solely* in order to acquire messages concerning names on the Watch Lists; those messages we acquire always are by-products of the foreign communications we intercept in the course of our legitimate and well recognized foreign intelligence activities.¹⁴⁰

Accordingly, he added “I believe that our current practice conforms to your guidance that, ‘relevant information acquired by you in the routine

and described “Liddy’s role: He is an expediter to breakdown bureaucratic problems by either grease or dynamite.” *Id.* at 113. Liddy was later convicted for his role in the Nixon Committee to Re-Elect the President’s efforts to break-in to Democratic Headquarters at the Watergate Hotel during the 1972 election. See Micheal Wines, *Tape Shows Nixon Feared Hoover*, N.Y. TIMES, June 5, 1991, at A20 (discussing Liddy’s conviction in connection with the Watergate scandal).

137. MCMILLAN, *supra* note 13, at 26–27.

138. S. REP. NO. 94-755, at 746 (1976).

139. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972).

140. Letter from Gen. Lew Allen, Dir., Nat’l Sec. Agency, to Elliot L. Richardson, Att’y Gen. of the United States (Oct. 4, 1973), available at <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB178/surv04.pdf>.

pursuit of the collection of foreign intelligence information may continue to be furnished to appropriate government agencies.”¹⁴¹

The agency also argued that communications that were obtained that were not relevant to the NSA’s foreign intelligence gathering purposes were discarded and that only relevant information was disseminated.¹⁴² For example, the agency emphasized that up to 97% of the international communications that were analyzed by computer or by human analysts was not retained.¹⁴³ However, even with this high rate of pruning (or, conversely, the low rate of “selecting out” communications of Americans), by the early 1970s the NSA’s analysts were reading over 150,000 telegrams to or from Americans each month under Operation SHAMROCK and analyzing an unrevealed quantity of radio communications of Americans that were “incidental” to the NSA’s other activities.¹⁴⁴ That is, due to the volume of communications the NSA was searching through for foreign intelligence information, even taking into account that only a small percent were read by NSA analysts, the effect was to intrude on the privacy of at least 100,000 Americans a month (assuming conservatively that some sent more than one telegram a month), or at least 1.2 million per year—and that was in the 1970s, before the Internet became widely used and Americans vastly expanded their reliance on electronic communications devices.¹⁴⁵

Project MINARET was ultimately terminated, but it is not clear to me that in the wake of the more recent revelations of activities by the Bush Administration that it was not subsequently reconstituted, expanded, and rebranded internally, as described more fully below. In the mid-1970s, a vigorous and skeptical Congress had thoroughly investigated Project MINARET and revealed that over numerous U.S. citizens or groups had been placed on NSA watch lists such that any communications by them or referencing them were sought out amid the pool of communications technologically available to the agency. And, beyond the watch list itself, General Allen told the Church Committee that the NSA had created and shared over 3,900 reports on watch-listed Americans.¹⁴⁶ And, at one point after the investigation had begun, he promised House Chairman Pike that the NSA was only targeting foreign-communications channels, which carried only a minuscule number of international communications by Americans, and was not “monitoring any telephone circuits terminating in the US.”¹⁴⁷

141. *Id.*

142. MCMILLAN, *supra* note 13, at 35.

143. *Id.* at 34. The NSA also emphasized that all personal communications involving Americans were discarded “at the earliest possible moment of discovery.” *Id.* at 35.

144. Bill Moyers Journal, *supra* note 54.

145. *Id.*

146. Allen, *supra* note 141.

147. See *FISA for the Future: Balancing Security & Liberty: Hearing Before the H. Perm. Select Comm. on Intelligence*, 110th Cong. 7–8 (2007) (statement of Lisa Graves, Deputy Director,

That is, the “one terminal” rule had been abandoned in order to protect Americans’ international communications, at least during the congressional investigation. And he asserted that once Operation SHAMROCK was shut down, the NSA was purportedly no longer analyzing the international telegrams of millions of American residents and businesses.¹⁴⁸

This snapshot of projects and operations terminated beliefs, to me, the truth. As discussed below, I think it is likely that some of the activities at the heart of SHAMROCK and MINARET continued in different ways with new internal “controls,” namely what was considered to be “incidental” collection involving Americans but that did not focus on Americans “intentionally” and did not permit the analysis of what was collected in this way. I think this is part of the “capacity” that was tapped by the Bush Administration with the aid of certain telecomm companies and with a new focus on the communications of Americans, as described below, to the detriment of our liberty and security. This shift in focus is of paramount importance and great consequence, constitutionally and morally, in our democracy.

III. Fast Forward to 2008: Undividing the World of Communications, Revising FISA, and Analyzing More Americans than Ever Before

What actually happened next is subject to tremendous debate, especially from the vantage point of the first decade of the 21st century. This much is mostly undisputed: in 1978, Congress passed FISA to regulate foreign intelligence surveillance on these shores, creating a special court to hear applications for warrants predicated on specially defined probable cause to engage in any surveillance that met the statute’s definition of “electronic surveillance.”¹⁴⁹ Congress created a comprehensive statute to govern this surveillance, explicitly stating that FISA and Title III were the “exclusive” rules for conducting these activities (and repealing the 1968 provision that had statutorily exempted the NSA from criminal penalties for warrantless electronic surveillance).¹⁵⁰ It set forth rules for emergency situations and times of war, providing that warrants were still required.¹⁵¹ It limited what counted as foreign intelligence so that the rationale for surveillance would not be as broad as President Nixon attempted to stretch foreign policy to

Center for National Security Studies) (citing a letter from Gen. Lew Allen, Dir., Nat’l Sec. Agency, to Hon. Otis G. Pike, Chairman, H. Select Comm. on Intelligence. (Aug. 25, 1975)).

148. *The National Security Agency and Fourth Amendment Rights: Hearing on S.R. 21 Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. (1975) (statement of Lew Allen, Jr., Director, NSA).

149. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 103–105, 92 Stat. 1783, 178–93 (codified as amended at 50 U.S.C. §§ 1803–1805 (2006)).

150. *Id.* § 201.

151. *Id.* § 105(e).

reach.¹⁵² Congress also wrote a special, broad definition of *content* to include not only the words spoken (like criminal wiretaps) but also the fact of communication, length of conversations, and the parties involved;¹⁵³ and then it referenced that content in the definitions of electronic surveillance, as explained below.¹⁵⁴

FISA barred warrantless targeting of communications to or from people in the United States whether by wire or radio and regardless of where the acquisition occurs (meaning even if not on these shores),¹⁵⁵ which sounds on the surface of the language like an attempt to bar Project MINARET's watch-listing. It barred warrantless acquisition of communications to or from Americans if acquired from a wire in the United States, even if not targeting a particular U.S. person.¹⁵⁶ This seems on the surface aimed at stopping the NSA from the bulk collection of the cables of telegram companies or other communications that traveled by wire to or from the United States, which seemingly describes SHAMROCK. FISA also barred the warrantless acquisition of purely domestic radio communications between people in the United States, and it barred other warrantless listening devices directed at people here in the United States.¹⁵⁷ This is, at least, what the plain language of the statute indicates.

To hear the Bush Administration and its proxies tell the story of FISA thirty years after the law passed, FISA changed nothing because the definitions cleverly exempted all of the NSA's SIGINT activities.¹⁵⁸ It is an astonishing claim. The implication of this construction of FISA is that the NSA was statutorily and constitutionally free to restart Project MINARET watch-listing so long as they did not search the pool of international communications for a particular American's *live* international communications by name, versus after the communication was transmitted, and that the NSA could re-engage Operation SHAMROCK so long as it moved the operation offshore.

Yet when President Jimmy Carter signed FISA into law in October 1978, he stated his belief that "The bill requires, for the first time, a prior judicial warrant for *all* electronic surveillance for foreign intelligence purposes in the United States in which communications of U.S. persons might be intercepted. It clarifies the Executive's authority to gather foreign

152. See Glenn Greenwald, *Echoes of the Nixon Era*, SALON, July 31, 2006, <http://www.salon.com/news/opinion/feature/2006/07/31/nsa> (characterizing FISA as a response to eavesdropping abuses by the Executive Branch, particularly under President Nixon).

153. FISA § 101(n).

154. *Id.* § 101(f)(1)–(2).

155. *Id.* § 101(f)(1).

156. *Id.* § 101(f)(2).

157. *Id.* § 101(f)(3).

158. The Bush Administration argued that an exception to FISA allowed the NSA to continue to gather surveillance on international radio communications without a warrant, claiming these were the majority of international calls. See *infra* notes 184–85 and accompanying text.

intelligence by electronic surveillance in the United States.”¹⁵⁹ Not that such statements are definitive by any means given our constitutional structure, but he also stated his belief that FISA

helps to solidify the relationship of trust between the American people and their Government. It provides a basis for the trust of the American people in the fact that the activities of their intelligence agencies are both effective and lawful. It provides enough secrecy to ensure that intelligence related to national security can be securely acquired, while permitting review by the courts and Congress to safeguard the rights of Americans and others.¹⁶⁰

Indeed, the Senate in its report on the bill noted that FISA “[was] designed . . . to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it.”¹⁶¹ The Senate said it passed FISA to “provide the secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation’s commitment to privacy and individual rights.”¹⁶²

One of the main points of recent disagreement surrounds the so-called radio exception from the definitions of FISA to not include non-targeted international radio transmissions in FISA’s warrant requirement.¹⁶³ But Congress made clear that the exclusion of some surveillance of Americans from FISA’s definitions “should not be viewed as congressional authorization of such activities as they affect the privacy interests of Americans,” noting that “the requirements of the [F]ourth [A]mendment would, of course, continue to apply to this type of communications intelligence activity,” regardless of FISA.¹⁶⁴ In fact, Congress envisioned that these activities would be governed by provisions in Senate Bill 2525,¹⁶⁵ but that bill never passed, and the White House issued an Executive Order and also internal rules, such as United States Signals Intelligence Directive 18, to further establish rules for the collection and dissemination of material that affected Americans’ privacy rights, beyond the statutory

159. Foreign Intelligence Surveillance Act of 1978, 2 PUB. PAPERS 1853 (Oct. 25, 1978).

160. *Id.*

161. S. REP. NO. 95-604, pt. 1, at 8 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3910.

162. *Id.* at 15.

163. *See Legislative Proposals to Update the Foreign Intelligence Surveillance Act (FISA): Hearing Before the H. Subcomm. on Crime, Terrorism, and Homeland Sec., Comm. on the Judiciary 109th Cong. 103 (2006) [hereinafter *Legislative Proposals*]* (statement of Jim Dempsey, Policy Director, Center for Democracy & Technology).

164. H.R. REP. NO. 95-1283, pt. 2, at 51 (1978); *see also* S. REP. NO. 94-1035, at 30 (1976); S. REP. NO. 94-1161, at 27 (1976) (indicating that the exclusion of certain types of surveillance from FISA did not indicate Congress’s approval of warrantless surveillance in those circumstances and noting the Fourth Amendment still applied to that surveillance).

165. National Intelligence Reorganization and Reform Act of 1978, S. 2525, 95th Cong. (1978).

protections.¹⁶⁶ Plus, Congress took pains in FISA's legislative history to emphasize that broadscale electronic surveillance, even of Americans who were abroad, had been limited by the Executive.¹⁶⁷ Congress stated that the statute intentionally barred the tapping of wire communications without a warrant for "either a wholly domestic telephone call or an *international* telephone call . . . if the acquisition of the content of the call takes place in this country . . ." ¹⁶⁸ And, in fact, FISA even provided special rules for a limited class of communications in the U.S. to permit warrantless electronic surveillance of special phone lines leased by foreign governments for their embassies here, by allowing the Attorney General to authorize such surveillance if there was "no reasonable likelihood" that Americans' communications would be intercepted through such orders without a warrant (this has been called the "embassy exception" or "leased-line rule").¹⁶⁹ The Act also restricted testing of radio surveillance equipment to prevent "testing" from being a backdoor way to direct the ears of the NSA at the United States.¹⁷⁰ And, among other things, it provided "minimization" rules to limit how information that was lawfully obtained in foreign intelligence collection could be retained and shared.¹⁷¹ These rules specifically mandated the destruction of Americans' communications if they were incidentally obtained without warrants as part of the leased-line exception to the warrant requirement, unless such communications contained information demonstrating a risk to life or limb, or a warrant was later obtained.¹⁷²

All of these restrictive provisions create the strong impression in the public that FISA prevented the warrantless electronic surveillance of Americans on these shores by the government in the name of foreign intelligence gathering.¹⁷³ Admittedly, some things were left out of FISA's comprehensive rubric that accorded different procedures to different things based on geography—that is, the geography of America and the rights to be accorded to Americans. But it is hard to fully credit the Bush-era argument

166. See *Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 11 (2007) [hereinafter *Modernization of FISA*] (statement of Kate Martin, Director, Lisa Graves, Deputy Director, Center for National Security Studies).

167. S. REP. NO. 95-604, pt. 1, at 34 n.40, reprinted in 1978 U.S.C.C.A.N. 3904, 3936.

168. *Id.* at 33.

169. See *Legislative Proposals*, *supra* note 172, at 106 (statement of Jim Dempsey, Policy Director, Center for Democracy & Technology) (explaining the embassy exception).

170. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511 § 105(f), 92 Stat. 1783, 1790 (codified at 50 U.S.C. § 1805 (2006)).

171. FISA § 101.

172. FISA § 101(h)(4).

173. That is not to say there were not gaps and flaws from a civil liberties standpoint, but it is to say that a fundamental precept of statutory interpretation is to give words their plain meaning and not to construe provisions as meaningless. See Daniel T. Ostas, *Legal Loopholes and Underenforced Laws: Examining the Ethical Dimensions of Corporate Legal Strategy*, 46 AM. BUS. L.J. 487, 517 n.99 (2009) (stating that statutory interpretation involves appeals to plain meaning as well as maxims of construction).

that Congress exempted out crucial, constitutional protections for Americans' rights in the wake of the visceral awareness of the dangers of unchecked electronic surveillance and mountains of evidence of privacy violations involving NSA's SIGINT activities.

It is clear, however, that the government did not shut down NSA's satellite surveillance of foreign radio communications, although it seems highly likely that there was an understanding that these powers would be focused elsewhere, such as on the Kremlin in the Soviet Union in the midst of the Cold War or on listening for ciphered and unciphered communications involving foreign troop or naval movements, etc. And, it seems clear to me that this foreign intelligence-gathering power and focus would not be directed toward the United States and that there were to be special rules to protect Americans whose communications were genuinely inadvertently acquired. In addition, there were rules that stated that the NSA analysts working in silos in stations around the world to de-channel and decipher radio signals would not focus on American communication channels or particular Americans and that American communications would be discarded unless relevant to genuine foreign intelligence gathering.¹⁷⁴ It seems, however, that something changed from those original understandings between the Carter Administration and the second Bush Administration, and it was not just the need to respond to 9/11. But, before we turn to that mystery, let us examine the claims made in the second Bush Administration about what FISA meant and why the law needed to be changed *after* it was revealed that the Bush Administration had issued directives that resulted in far more American communications being analyzed by the NSA than apparently was the practice before then.

A. *"Almost All Local Calls Were on a Wire and Almost All Long-Haul Communications Were in the Air"—A Partial Truth Hiding the Whole Truth*

Once the Bush Administration decided to change the debate over the PP to attempting to get Congress to ratify and expand the new electronic surveillance activities it had undertaken, it cleared a set of public talking points to rationalize, indeed normalize, what it had done and then some. A key element of this argument was the claim that FISA permitted the NSA to engage in warrantless electronic surveillance of Americans' international radio communications, and Americans' international communications occurred via wire, rather than wirelessly, so Congress needed to ratify NSA access to wired communications.¹⁷⁵ For example, Admiral Michael

174. FISA § 101(h)(1).

175. See *Modernization of FISA*, *supra* note 175, at 6 (statement of J. Michael McConnell, Director of National Intelligence) (arguing that "FISA's definitions of 'electronic surveillance' should be amended so that it no longer matters how collection occurs (whether off a wire or from the air)").

McConnell, who was then the Director of National Intelligence, testified that when FISA was passed “in 1978, almost all local calls were on a wire and almost all long-haul communications were in the air, known as ‘wireless’ communications,”¹⁷⁶ but now “the situation is completely reversed; most long-haul communications are on a wire and local calls are in the air.”¹⁷⁷

However, as noted earlier, in contemporaneous disclosures within the Executive Branch that have now been declassified, the NSA in 1976 described quite clearly that almost all domestic calls were a combination of wire and microwave¹⁷⁸ (“in the air,” and even called “wireless” by the NSA back in the day).¹⁷⁹ And although the NSA’s focus had indeed been monitoring high-frequency radio waves that traveled across the globe, it is clear that there were other international communications that it could *not* intercept that way. Operation SHAMROCK is a case in point. In that secret, unconstitutional program, the millions of telegrams the NSA had been accessing—and then analyzing by hand at a rate of 150,000 a month in the mid-1970s—were transmitted via cable, i.e., wire.¹⁸⁰ And the historical record shows that a substantial portion of international calls to or from Americans transited the ocean via undersea cables, not via radio waves beamed to the sky.¹⁸¹ Some international calls of Americans travelled via satellite, but many travelled via cable.¹⁸² And foreign-to-foreign communications across Europe and Asia were most likely partly carried by wire and partly radio waves.¹⁸³ That is, through the use of satellite surveillance, it was not as though the NSA had access to every single telephone call on the globe, just the portion that travelled by high-frequency radio waves, if the signal were captured and de-channeled and recorded. This surveillance took place before the recent era of infinitely smaller electronic storage capacity; it is almost impossible to believe that the NSA was storing every single radio signal beamed from anywhere on the planet since 1978. That simply cannot be the case, from an effectiveness standpoint or as a practical matter, let alone a legal matter. At a minimum, post-FISA, the NSA was not supposed to be focusing on the U.S. and acquiring

176. *Id.* at 3.

177. *Id.* at 4.

178. Microwaves actually travel at a higher frequency, and in straight lines, than what is known as high-frequency radio, which follows the curvature of the earth. MCMILLAN, *supra* note 13, at 131.

179. *Id.*

180. *Id.* at 32.

181. *Modernization of FISA*, *supra* note 175, at 187 (statement of Kate Martin & Lisa Graves, Center for National Security Studies).

182. *Id.*

183. The transmission of intercontinental communication usually involved more than one medium. See Arthur E. Kennelly, *Recent Technical Developments in Radio*, 142 ANNALS AM. ACAD. POL. & SOC. SCI. 8, 9 (1929) (describing the process of transmitting a communication between the United States and England as involving the transmission of signals via radio waves and wire).

Americans' purely domestic radio signals, and it had to have a way of *not* doing that even if it had the capacity to do collect all radio signals in the world.

But the more important distinction, and history confirms, is that radio was the dominant medium for foreign governments to communicate with their ships and subs at sea, their planes in the air, and often with their embassies abroad.¹⁸⁴ And it is *that* core defense-related activity which Congress primarily intended to preserve in FISA, not to offer the NSA a huge loophole for collecting and analyzing Americans' private communications in the aftermath of condemning the NSA for doing just that.¹⁸⁵ The carve out was designed to allow the NSA to monitor, for example, the USSR's communications with its sailors, soldiers, airmen, and diplomats; it was not designed to focus on Americans,¹⁸⁶ whom Congress believed had legitimate privacy interests in their communications that necessitated a warrant for targeting Americans and other kinds of electronic acquisition of their private, personal communications.¹⁸⁷

Still, for that portion of Americans' international calls that were acquired as part of what was the NSA's foreign, as opposed to domestic, focus it seems clear from the historical record that some Americans' international calls were "incidentally" intercepted, that is, inadvertently, not intentionally.¹⁸⁸ What this means is that the U.S. channels were not supposed to be the focal point of the NSA's activities, but that in the physical process of receiving radio waves some would be intercepted, and internal rules then determined whether they would be de-channelled and listened to. And, I submit that the norm was—or at least was intended to be in the immediate aftermath of the Church Committee—that the NSA would not turn this

184. Communications to embassies were often enciphered and on specific channels—and you can see evidence of this reliance to this day around Washington with the little satellite dishes and radio towers on many embassies. See David Kahn, *The Rise of Intelligence*, 85 FOREIGN AFF. 125, 130–32 (2006) (providing a history of military intelligence, noting the importance of radio communication between governments and their submarines, planes, and military bases).

185. See S. REP. NO. 94-1035, at 19 (noting that electronic surveillance under the FISA bill "would be limited to 'foreign powers' and 'agent of a foreign power,' with American citizens being subject to the surveillance only if acting 'pursuant to the direction of a foreign power' and engaging in certain designated activities . . .").

186. See 50 U.S.C. § 1802(a) (2006) (permitting electronic surveillance without a court order so long as the Attorney General certifies that such surveillance is directed at communications "between or among foreign powers" with no "substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party").

187. See 123 CONG. REC. S7857 (daily ed. May 18, 1977) (statement of Sen. Kennedy) ("Electronic surveillance can be a useful tool for the Government's gathering of certain kinds of information; yet, if abused, it can also constitute a particularly indiscriminate and penetrating invasion of the privacy of our citizens.").

188. See Bob Woodward, *Messages of Activists Intercepted*, WASH. POST, Oct. 13, 1975, at A14 (according to Woodward's sources "the NSA [intercepted] all kinds of irrelevant communications, some involving U.S. citizens" prior to FISA).

incredibly intrusive weapon of surveillance on American channels even though it had the technical capacity to do so.

This makes perfect sense if we consider what radio meant in 1978. Whether referring to the thousands and thousands of high-frequency foreign calls travelling along the curvature of the earth, or lower frequency radio signals from an FM station, the essence of radio is that if you have a powerful enough receiver you can tune into a particular channel (and listen to it or record it for later), just like with a short-wave radio, the radio in your car or a transistor radio at the beach.¹⁸⁹ For multi-channel radio, which phone companies used to handle the volume of domestic and international calls that were not transmitted by wires or were partly transmitted by radio waves, the signal must be de-channelled to listen to it.¹⁹⁰ Why this matters is that some channels were more likely to be purely foreign communications—within a foreign country, between countries or from a country's capitol to its military or diplomats—and encoded, while other channels were more likely to be American channels, either purely domestic or international.¹⁹¹

To carry the analogy further, some telephone channels operate almost like a station that plays rock-n-roll all the time while other channels operate like community radio with a variety of programming. If you were charged with gathering foreign intelligence, the heart of which was foreign policy and matters of war and peace, you would be likely to tune out certain channels and very likely to tune in others. If your receivers were large or strong or precise enough, in effect, you might very well have the technical capacity to listen to Americans' domestic calls from New York to Los Angeles.¹⁹² And, you would also have to make decisions about whether you were going to record or retain all those radio waves bouncing across the earth. If your focus were the Soviet Union during the Cold War, for example, you might listen quite actively (around the clock) from your NSA stations around the

189. See MCMILLAN, *supra* note 13, at 131 (noting that “unsophisticated radio receivers over an area of perhaps 30 per cent of the earth’s surface” could intercept the radio portion of international radio-telephone communications to the United States and that “[h]igh frequency multi-channel transmissions may be de-channelled by ‘home made’ amateur equipment”).

190. See *supra* notes 124–26 and accompanying text (explaining that high-frequency radio signals could be intercepted and de-channelled); see also DUNCAN CAMPBELL, INTERCEPTION CAPABILITIES 2000 (1999), available at http://www.cyber-rights.org/interception/stoa/ic2kreport.htm#N_16_ (noting in a report to the Director General for Research of the European Parliament that “[h]igh frequency radio signals are relatively easy to intercept” and that “[f]rom 1945 until the early 1980s, . . . NSA . . . operated [high-frequency] radio interception systems tasked to collect European [International Leased Carrier] communications in Scotland”).

191. See CAMPBELL, *supra* note 190 (relating that the NSA used high-frequency radio monitoring systems, including ones which could “simultaneously intercept and determine the bearing of signals from as many directions and on as many frequencies as may be desired,” to intercept Soviet and Warsaw Pact air force communications, French diplomatic communications, and diplomatic messages sent to and from Washington).

192. See MCMILLAN, *supra* note 13, at 131 (describing the wireless component of the United States commercial communication system as “a multi-channel microwave carriers system capable of carrying up to 2,000 communications on some channels”).

world, staffed with linguists, to certain channels and record them for later analysis to search for certain code words or information, but if you were rational you probably would not devote staff to listening to radio transmissions from Des Moines to Denver and you probably would not record it; and even if you did accidentally collect it and record it you probably would not keep it forever. And, you certainly would not listen to wireless communications between Denver and Des Moines, if doing so were barred.

Under this conceptualization, the focus of the NSA's activities is better conceived of as foreign not international. And the bulk of those purely foreign communications focused upon for "foreign intelligence" gathering would likely not involve Americans at all.

B. What If Most Digital Communications Accessible Involved Americans?

Just to be clear, it was emphatically *not* the case that almost all domestic calls of Americans were by wire and almost all international calls were wireless in 1978.¹⁹³ And, so, it is not the case that giving the NSA warrantless access, as has been alleged in sworn statements, to the digital network—that is the digital backbone of the U.S. communication system—is balancing the scale to restore what was supposedly permitted in 1978. It is breaking the scale. Even if this were the tacit arrangement embodied in the FISA Amendments Act and subject to new internal "controls," then just as David Kris, who is now the Assistant Attorney General for the National Security Division, previously urged that "current policymakers should not be prisoners to the judgments of 1978,"¹⁹⁴ we should not be prisoners of the judgments of 2008 or the judgments of 2001.

There is some evidence that the NSA pressed for access to the digital communications network as part of briefing the transition teams for incoming President George W. Bush.¹⁹⁵ And there is some evidence that the Bush Administration asked the major telephone companies for a new kind of access to their digital network before September 11th,¹⁹⁶ a request which

193. See *Modernization of FISA*, *supra* note 175, at 187 (statement of Kate Martin & Lisa Graves, Center for National Security Studies) (contending that when FISA was passed, it was not true that all international calls were via satellite radio and all domestic calls were via wire).

194. David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: A Working Paper of the Series on Counterterrorism and American Statutory Law* 7–13 (Brookings Inst., Geo. Univ. Law Center, & Hoover Inst., Paper No. 1, 2007), available at http://www.brookings.edu/~media/Files/rc/papers/2007/1115_nationalsecurity_kris/1115_nationalsecurity_kris.pdf.

195. See NSA, TRANSITION 2001 32 (2000), available at <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa25.pdf> (urging the Bush Administration to allow the NSA to have a "permanent presence on a global telecommunications network").

196. See Scott Shane, *Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11*, N.Y. TIMES, Oct. 14, 2007, <http://www.nytimes.com/2007/10/14/business/14qwest.html> (reporting that Qwest Communications refused an NSA proposal that Qwest considered illegal in February 2001).

Qwest Communications reportedly denied and subsequently lost favorable treatment by the federal government on other matters, as indicated in statements made by their CEO during his prosecution for insider trading.¹⁹⁷ But, it is also clear that in the fall of 2001, new directives were issued by President Bush that had the effect of expanding what the NSA was doing with its technological capacity and that seemingly affected how U.S.-based telecommunications companies cooperated with the government in response, at least according to public affidavits sworn under penalty of perjury.¹⁹⁸ That evidence demonstrates that, technologically, the NSA was making duplicates of the digital communications within the United States, and not doing so at the bulkheads of the fiber-optic network going into and out of the United States, but at a variety of locations within the United States, on systems that commingled the domestic and international conversations and e-mails and all related data of Americans in the communications packets passing through the fiber optic network literally at the speed of light.¹⁹⁹

But, setting that aside for now, I want to look at whether the Bush Administration's legal rationale for expanded access to the U.S. communications grid, pre- or post-9/11, is strong and comports with legal precedent and wise policy analysis. I confess that my skepticism is deepened, in part, by the widely condemned results-oriented legal analysis of John Yoo, who wrote the initial rationales for the PP and other controversial secret programs, and his ideological predisposition toward expanding executive power.²⁰⁰ It also is informed by the systematic attempt in the "white paper" the Justice Department produced in January 2006 (which I call the kitchen sink memo) to posit alternative rationales for the PP and to limit

197. *Id.*

198. See Peter Baker, *President Acknowledges Approving Secretive Eavesdropping*, WASH. POST, Dec. 18, 2005, <http://www.washingtonpost.com/wp-dyn/content/article/2005/12/17/AR2005121700456.html> (reporting that an intelligence official confirmed that Bush signed an order authorizing the NSA surveillance program in October 2001, not in 2002 as previous reports had indicated).

199. See Susan P. Crawford, *Transporting Communications*, 89 B.U. L. REV. 871, 928 (2009) ("In fiber-optic installations, strands of glass no thicker than a human hair allow pulsing photons to move across them at speeds close to the speed of light . . ."); *id.* at 898–900 (explaining that communications services are mostly based upon the Internet Protocol, which is a "common language allowing the division of all communications into small packets that are then individually routed, one hop at a time, to their destination"); Shayana Kadidal, *Does Congress Have the Power to Limit the President's Conduct of Detentions, Interrogations and Surveillance in the Context of War?*, 11 N.Y. CITY L. REV. 23, 56 n.123 (2007) (indicating that with the advent of digital telephony, phone calls are moved along "the fiber optic backbones of the major phone carriers . . . in much the same manner as internet packets are moved").

200. See Pamela Hess & Lara Jakes Jordan, *Memo Linked to Warrantless Surveillance Surfaces*, USA TODAY, available at http://www.usatoday.com/news/washington/2008-04-03-surveillance-memo_N.htm (reporting that federal documents indicate that an October 2001 internal memorandum written by John Yoo related to the PP, although a White House spokesman said the memo did not form the basis for the program). See generally John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565 (2007) (arguing for the legality of the PP).

the reach of the warrant requirement that was at the heart of FISA's definitions.²⁰¹ That is to say, at key junctures, the Bush Justice Department took an expansive reading of executive power and a parsimonious, hair-splitting view of the privacy and civil liberties at stake. And it squeezed Congress to accept these constrained views.

For example, the Bush Justice Department repeatedly emphasized their view that, for the government to listen to Americans' conversations warrants were not constitutionally required in foreign intelligence surveillance;²⁰² that federal law setting warrants as a requirement to conduct certain types of surveillance was not binding;²⁰³ that for conversations already obtained, the appropriate standard is derived from the "special needs" cases and that reasonableness is the operative test;²⁰⁴ that the reasonableness test could be satisfied solely by the President's determination;²⁰⁵ and finally, that courts should not be permitted *even the possibility* of ruling against the President's determination.²⁰⁶

As for communications *data*, the Bush Administration emphasized repeatedly its view that there is no constitutional interest at stake²⁰⁷ and they have therefore kept hidden the number of Americans whose communications data has been obtained.²⁰⁸ And they have asserted similarly that Americans

201. U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (2006).

202. *See id.* at 7 (arguing that there is an understanding that the President does not need a warrant for foreign intelligence surveillance, even in the United States).

203. *See id.* at 20–23 (asserting that FISA does not apply where surveillance is authorized by another federal statute).

204. *See id.* at 37–39 (arguing that the special needs doctrine renders the Fourth Amendment warrant requirement inapplicable to the NSA activities).

205. *See id.* at 40 (explaining that "the President has stated that the NSA activities are 'critical' to our national security," and urging that this governmental interest can overcome individual privacy interests under the balancing of interests analysis used to determine reasonableness).

206. *See id.* at 35 (arguing that an interpretation of FISA that would not allow the President to conduct the NSA activities "would be unconstitutional as applied in the context of this congressionally authorized armed conflict"); *id.* at 36 & n.21 (contending that if the AUMF were not construed to be a statute authorizing electronic surveillance outside FISA procedures in accordance with the exclusivity provision added by FISA, then "[t]he President's determination that electronic surveillance of al Qaeda outside the confines of FISA was 'necessary and appropriate' would create a clear conflict between the AUMF and FISA" and that such conflicts should be avoided).

207. *See Risen & Lichtblau, supra* note 98 (explaining that, when confronted with criticism about the constitutional implications of its communications data surveillance programs, "Bush administration officials argue[d] that the civil liberties concerns [were] unfounded . . ."); Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 *FORDHAM L. REV.* 1731, 1733, 1738–39 (2006) (explaining the Bush Administration's reliance on the "third-party doctrine"—the principle that "when we convey information to a third party, we give up all constitutionally protected privacy in that information"—to help justify its data-surveillance programs, despite the statutory protections that had been created).

208. They have done so in this context and for National Security Letter disclosures under § 505 of the USA Patriot Act as amended. *See* Dan Eggen, *Spy Chief Discloses Broader Program*, *WASH. POST*, Aug. 1, 2007, at C3 (describing the Bush Administration's refusal to confirm news reports that it had obtained millions of Americans' phone records from telecommunication companies);

have no cognizable constitutional interest in information a person turns over to a company, be it financial records or Internet transactions.²⁰⁹ So, should Americans assume that the NSA is now capturing their all communications data and analyzing it for the indefinite future, under the notion that we do not have any cognizable constitutional interest in keeping this private from the government's prying eyes?

The problem is not that there is no case law to analyze and extrapolate from. The problem is that there was no apparent effort to assess whether doing X rather than Y was a good idea, whether that older case law comports with modern realities, or what the genuine implications are for Americans' privacy and liberty interests. It seems decisions were viewed, and continue to be viewed, through the lens of Vice President Cheney's "one percent doctrine," the ultimate ends-justify-the-means rationale.²¹⁰ So please forgive me for being jaded about whether they got the balance right in FISA or other areas.

In essence, the legal argument seems to have boiled down to one word: terrorism. And, as demonstrated by the faulty FISA Court of Review decisions, substituting the reasonableness test for the warrant requirement results in no warrant being required to acquire increasing volumes of communications, including Americans' communications.²¹¹ And no warrant has apparently been required to drill down into the primordial soup of these communications—to compile detailed information about Americans' communications. These communications involve everything from the mundane to the intimate: their freedom of conscience, freely expressed, via e-mail or text or digital calls that can now be much more easily recorded, saved, and indefinitely searched and analyzed by this presidential administration and future Executive Branch leaders in the decades to come.

All that is to say that the revolution in digital communications and communication patterns—which served as one of the rationales for the push to change FISA to permit more warrantless electronic surveillance²¹²—

Daniel Klaidman, *Now We Know What the Battle Was About*, NEWSWEEK, Dec. 22, 2008, at 46 (discussing the NSA's collection and storage of "the records of calls and e-mails of tens of millions of average Americans between September 2001 and March 2004," and noting the Bush Administration's unwillingness to comment on or provide information about the program).

209. See, e.g., Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third Party Information, Third Parties and the Rest of Us Too*, 34 PEPP. L. REV. 975, 977–82 (2007) (exploring how the third-party doctrine was used to justify the NSA's and FBI's warrantless surveillance of emails and banking records).

210. RON SUSKIND, *THE ONE PERCENT DOCTRINE* 62 (2007) (describing Cheney's formulation of the one percent doctrine).

211. Stephanie Cooper Blum, *What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 282 (2009) (describing the FISA Court of Review's conclusion that a FISA Amendments Act "warrant," what is really an order permitting a program of surveillance without any of the indicia of a Fourth Amendment warrant, should be granted unless the government's sole objective was to obtain evidence of a past crime).

212. This was one of the arguments made by the Director of National Intelligence and the expensive lobbyists of the phone companies that were trying to prevent legal liability for

actually warrants *greater* privacy protections for Americans, not *weaker* ones. And, it is my view that greater privacy protections for Americans will help ensure that precious anti-terrorism resources and Americans' precious tax dollars are not squandered capturing, storing, and analyzing innocent Americans. These tools, this *weapon* of surveillance capacity to capture almost every electronic conversation one has and all the data about who our friends and family are, should not be turned on Americans.

As I have noted in my previous testimony with Kate Martin:

[B]y any reasonable estimate of the number of actual suspected al Qaeda operatives in contact with the US, the volume of innocent communications of Americans that would be swept up in a nation of 300,000,000 people creates a ratio exponentially smaller than even the so-called one percent doctrine of the Vice President. Statistically, the proportion of innocent international calls and e-mails that would be statutorily allowed to be vacuumed under [the then-proposed amendments to FISA] would be on the order of 99.999+ innocent—and, at what cost in both privacy and money? There is no such exception in the Fourth Amendment. The Constitution does not permit the seizure of millions or billions of conversations or e-mails of Americans to look for a few.²¹³

Ultimately, FISA was changed, in response to national security fear-mongering by President Bush, to permit warrantless access from within the United States of electronic communications in which at least one party to the communication is reasonably believed to be located outside the United States (resurrecting the one-terminal rule that had been cut back by FISA initially, at least for communications acquired in the United States) if the goal of collecting the communications is to obtain foreign intelligence.²¹⁴ Let us consider what may be possible under the new rules and rationales. And let us consider what additional information it would be important to know to assess this.

IV. What Does “Incidental” Collection Mean Under FISA as Amended With Current Technology and What About “Intentional” Collection and/or Analysis of Americans’ Conversations and Communications Without Warrants?

One of the keys to understanding what this new warrantless surveillance means for American privacy is to revisit what then-NSA Director General Hayden reportedly told the Bush Administration in 2001 about the NSA’s

cooperating with the Bush Administration’s breach of FISA’s rules. *See Modernization of FISA*, *supra* note 175, 18 (statement of J. Michael McConnell, Director of National Intelligence).

213. *Modernization of FISA*, *supra* note 175, at 187 (statement of Kate Martin & Lisa Graves, Deputy Director, Center for National Security Studies).

214. The FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702(a), 122 Stat. 2436 (to be codified at 50 U.S.C. § 1881(a)).

capabilities. It is also useful to revisit what this means for American's privacy in light of the NSA rationales in the declassified McMillan memorandum.

Following September 11th, General Hayden took immediate actions in response to al Qaeda. In Hayden's testimony to the Senate Intelligence Committee, he stated that he was then asked by other Bush Administration officials "[i]s there anything more you can do? And I said, 'not within my current authorities.'"²¹⁵ He then described three ovals of a Venn Diagram as "what was technologically possible, what was operationally relevant, and what would be lawful."²¹⁶ According to John Yoo's book, which reiterates this story, the administration argued that the President as Commander in Chief had the authority to take any action he deemed lawful,²¹⁷ meaning that the overlapping "lawful" oval of NSA activities in the diagram could be expanded at will. As the administration re-interpreted expansive authority of the President to act outside of federal statutes, construed prior executive orders as nonbinding, and (as discussed above) interpreted the Fourth Amendment narrowly to encompass only a reasonableness test for electronic surveillance, they greatly exceeded the boundaries established previously.

When General Hayden testified to the Senate during his CIA Director confirmation hearing, he was asked about whether there were privacy concerns for Americans swept in by the program. Hayden told the Senate:

[F]rom the very beginning, we knew that this was a serious issue, and that the steps we were taking, although convinced of their lawfulness, we were taking them in a regime that was different from the regime that existed on 10 September. I actually told the workforce . . . free peoples always hav[e] to decide the balance of security and their liberties, and that we through our tradition have always planted our banner way down here on the end of the spectrum toward security. And then I told the workforce—and this has actually been quoted elsewhere—I told the workforce there are going to be a lot of pressures to push that banner down toward security, and our job at NSA was to keep America free by making Americans feel safe again. So this balance between security and liberty was foremost in our mind.²¹⁸

When pressed about whether there were privacy concerns involved in the PP, meaning were *Americans'* rights implicated, General Hayden

215. *Nomination of General Michael V. Hayden, USAF, to be Director of the Central Intelligence Agency: Hearing Before the S. Select Comm. on Intelligence*, 109th Cong. 28 (2006) [hereinafter *Hayden Nomination*] (statement of General Michael V. Hayden, General, U.S. Air Force).

216. *Id.* at 29.

217. JOHN YOO, *WAR BY OTHER MEANS* 103 (2006).

218. *Hayden Nomination*, *supra* note 225, at 29 (statement of Michael V. Hayden, General, United States Air Force).

responded, "I could certainly understand why someone would be concerned about this."²¹⁹

Shortly after the December 2005 story broke about the NSA's new activities, President Bush admitted to a single aspect of the PP, which he branded the "Terrorist Surveillance Program" (TSP), which involved listening to calls between any suspected al Qaeda agent and anyone in the United States.²²⁰ But, soon there was more confirmation that there were other aspects the President did not disclose that did not involve just listening to suspected terrorists. In the intervening period, General Hayden gave a public speech at the National Press Club in which he discussed the TSP, asserting:

It is not a driftnet over Dearborn or Lackawanna or Fremont grabbing *conversations* that we then sort out by these alleged keyword searches or data-mining tools or other devices that so-called experts keep talking about. This is *targeted* and focused. This is not about intercepting *conversations* between people in the United States. This is hot pursuit of communications entering or leaving America involving someone we believe is associated with al Qaeda. We bring to bear all the technology we can to ensure that this is so.²²¹

A few months after this, investigative reporters noted that sources had confirmed that the NSA's new activities included the data-mining of Americans' domestic calls and e-mails.²²² And shortly afterwards, President Bush nominated Hayden to head the CIA.²²³ At his confirmation hearing, Hayden was asked how to square the more recent reports with his press club remarks, and he stated that he chose his words carefully, adding:

I bounded my remarks by the program that the President had described in his December radio address. It was the program that was being publicly discussed. And at key points in my remarks I pointedly and consciously down-shifted the language I was using. When I was talking about a drift net over Lackawanna or Fremont or other cities, I switched from the word "communications" to the much more specific and unarguably accurate conversation. And I went on in the speech and later in my question and answer period to say we do not use the content of communications to decide which communications we want to study the content of. In other words, when we look at the content of the communications, everything between "hello" and "good

219. *Id.* at 33.

220. *Bush Says He Signed NSA Wiretap Order*, CNN, Dec. 17, 2005, <http://www.cnn.com/2005/POLITICS/12/17/bush.nsa/index.html>.

221. Heather Greenfield, *CIA Nominee's Hearing May Focus on Wiretapping*, GOVERNMENT EXECUTIVE, May 8, 2006, <http://www.govexec.com/dailyfed/0506/050806tdpm1.htm> (emphasis added) (quoting General Hayden's speech at the National Press Club).

222. See Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 10, 2006, at A1.

223. *Id.*

bye” we had already established a probable cause standard—right to a probable cause standard that we had reason to believe that that communication, one or both of those communicants were associated with al Qaeda.²²⁴

So, what this means is that once the restraint of the law was taken off the table, meaning FISA’s rules and related rules had been bent or broken by executive fiat, as of October 6, 2001, the Administration directed the NSA to analyze Americans’ call records and presumably their e-mail contacts as well. Here’s how Senator Carl Levin described the situation based on what was in the *public* record:

After listening to the Administration’s characterizations for many months, America woke up last Thursday to the *USA Today* headline, quote, “NSA has massive database of Americans’ phone calls.” The report said that “The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans The NSA program reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans—most of whom aren’t suspected of any crime.”

. . . . And the May 12 *New York Times* article quotes “one senior government official” who “confirmed that the N.S.A. had access to records of most telephone calls in the United States.”

We are not permitted, of course, to publicly assess the accuracy of these reports. But listen for a moment to what people who have been briefed on the program have been able to say publicly. Stephen Hadley, the President’s National Security Adviser, . . . said the following: “It’s really about calling records, if you read the story: who was called when, and how long did they talk? And these are business records that have been held by the courts not to be protected by a right of privacy. And there are a variety of ways in which these records lawfully can provided to the government . . . it’s hard to find the privacy issue here.”

Majority Leader Frist has publicly stated that the “program is voluntary.” And a member of this committee has said: “The President’s program uses information collected from phone companies—the phone companies keep their records. They have a record. And it shows what telephone number called what other telephone number.”²²⁵

So, it is clear that the program involved analyzing the connections among Americans, and between Americans and others, meaning the analysis

224. *Hayden Nomination*, *supra* note 225, at 50–51 (statement of Michael V. Hayden, General, United States Air Force).

225. Press Release, Sen. Carl Levin, Statement by Senator Carl Levin on the Nomination of General Michael Hayden for Director of the Central Intelligence Agency (May 18, 2006), <http://levin.senate.gov/newsroom/release.cfm?id=255787>.

of the communications of hundreds of millions of Americans—innocent Americans.

But, let us understand what this really means as a technological matter. As noted in the McMillan Memo, the NSA does not conceive of its activities as driftnets over particular cities or even as targeting particular Americans.²²⁶ It considers its activities to be “the routine pursuit of the collection of foreign intelligence information.”²²⁷ But, the Bush Administration basically redefined the pursuit of foreign intelligence information to include the analysis of purely domestic communications. That had been legally verboten, even if it had been technically feasible through the NSA’s technological ears. What the Bush Administration did was turn those ears inward or invite those ears to focus on U.S. communications—it made those communications “operationally relevant.” So, what was rationalized by the NSA in the McMillan Memo as the acceptable “inadvertent” or “incidental” collection of some number of Americans’ telephone calls that were minimized—meaning shared by name only if containing foreign intelligence information—has become no longer incidental, accidental, or inadvertent in the true sense of the words. The focus on the United States is intentional and deliberate. This is a major change. It is an enormous shift in mission. And it poses tremendous risks to liberty.

Here is one of the reasons why. As a technological matter, communications data travels in packets with content.²²⁸ This means that, in essence, the act of capturing a specific piece of data captures the content. So, unless the NSA were *only* obtaining Americans’ phone bills after the fact, as opposed to during the process of transmission, it is likely capturing the words spoken or written or texted are captured as well. Now it is certainly possible that there is some mechanism by which the NSA may be able to peel off the data and delete the text forever, but we must question whether any government agency should be given such access to the content of our conversations in a free society, without individualized suspicion and an independent check for probable cause of intentional wrongdoing.²²⁹ In other settings, General Hayden has asserted that any actual conversations that are obtained that do not have “inherent foreign intelligence value” are

226. See MCMILLAN, *supra* note 13, at 81, 82 (describing the NSA’s “one-terminal rule,” as a self-imposed restriction aimed at maintaining the agency’s focus on international intelligence, as well as its commitment to the protection of “individual constitutional rights and civil liberties,” by prohibiting the intentional interception of “a communication unless at least one terminal is outside the United States”).

227. *Id.*

228. See, e.g., INTERNET ENGINEERING TASK FORCE, INTERNET PROTOCOL: DARPA INTERNET PROGRAM PROTOCOL SPECIFICS 11 (1981), available at <http://tools.ietf.org/html/rfc791> (establishing the IPv4 protocol, which is the foundation for the Internet, and specifying the source, destination, and other transmission information that must be included in each header of a data packet).

229. Some legal scholars have argued that true anonymization and minimization is impossible. See Paul Ohm, *Law in a Networked World: Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1.

“suppressed,” his technical description of how the agency engages in the “minimization” of conversations, in addition to expunging the identities of Americans when transcripts of conversations are circulated.²³⁰ But what does suppression of the digital records of e-mails and phone calls mean? It seems too complicated a way to describe “destruction,” and instead seems like a clever way to describe the *retention* of the material and the potential for analysis of it, indefinitely. But, let’s examine what this may mean in the context of the FISA Amendments Act (FAA).

The FAA permits the FISA Court to issue orders approving programs of surveillance and it is described as covering NSA “acquisitions” in which one party is reasonably believed to be outside the United States (the one-terminal rule) and the objective is to obtain foreign intelligence information.²³¹ But, the NSA’s position, as made manifest by the McMillan Memo, is that its collection of international communications, meaning purely foreign as well as Americans’ international conversations, is in pursuit of foreign intelligence information.²³² In fact, that is also how it described Operation SHAMROCK—that it was searching the international cables of American residents and businesses for foreign intelligence information.²³³ The NSA’s core business is pursuing foreign intelligence information.²³⁴ So, with respect to domestic communications, the NSA may have taken the view that domestic call and e-mail records are operationally relevant in pursuit of connections to foreign nationals. That is, an American’s call records and Internet transactions *may* reveal their connections to people abroad.²³⁵ How

230. General Michael V. Hayden, Principal Deputy Dir. of Nat’l Intelligence, Office of Nat’l Intelligence, Address to the National Press Club: What American Intelligence & Especially The NSA Have Been Doing To Defend The Nation (Jan. 23, 2006) (transcript available at http://www.dni.gov/speeches/printer_friendly/20060123_speech_print.htm).

231. FISA Amendments Act of 2008, § 703, Pub. L. No. 110-261, 122 Stat. 2436 (to be codified in 50 U.S.C. § 1881b).

232. See MCMILLAN, *supra* note 13, at 26–27 (explaining the NSA surveillance program MINARET, which selected “certain by-product intelligence” from foreign intelligence sources, and asserting that, “NSA dealt only with ‘foreign communications’, i.e., communications having at least one terminal on foreign soil”).

233. S. REP. NO. 94-755, at 733–34 (1976) (“With one exception, NSA contends that its interceptions of Americans’ private messages were . . . for ‘foreign intelligence’ purposes. This contention is borne out by the record.”).

234. See *infra* notes 244–42.

235. See generally David E. Pozen, Note, The Mosaic Theory, National Security, and the Freedom of Information Act, 115 YALE L. J. 628, 630 (2005) (“The ‘mosaic theory’ describes a basic precept of intelligence gathering: disparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information.”). The legal validity of this theory and data mining in this context has been challenged by civil liberties advocates, including me. The embrace of this theory dramatically changes the rules for protecting the rights of individuals because it attempts to rationalize and normalize the collection of information that is, by definition, not relevant and the retention of information that is not relevant under the notion that it may some day be relevant (in essence conceding that it is not currently relevant). This theory’s circularity is deeply problematic when it comes to Americans’ interests in privacy and liberty. We have seen this argument repeatedly from the FBI, including General Counsel Valerie Caproni, among others, who claimed in meetings with

will the NSA find out about those connections without tracking such records in the first place? This is the very circularity of such an approach.

Today, when one looks at the FAA definitions, they read more like swords than shields, as we know now how the Executive Branch, and the NSA, has interpreted its powers over time. For example, in pursuit of foreign intelligence under this statutory authority, purely domestic conversations are subject to a warrant requirement only if the NSA knows *at the time of acquisition* that the sender and all recipients are in the United States.²³⁶ What does this mean now for genuinely domestic e-mails or phone calls—how does the NSA *know* where the sender and all the recipients are when it is duplicating communications transiting the fiber optic network. If the agency does not know that you and everyone you are e-mailing are in the United States rather than on spring break in Paris or Cancun at the time the e-mail is sent, does it presume the communications are fair game for acquisition and analysis?

When previously pressed on this issue, the Bush Administration through its proxies, in essence, claimed that it did not know for certain that an American area code is being used in America or that an American is not accessing his or her e-mail from an internet café abroad. And the rules for purely domestic *conversations* seem quite apart of *communications*, in the words of General Hayden.²³⁷ So, while there now appears to be FISA Court orders to permit certain kinds of access to communications in the United States, that does not mean that the only communications being acquired and

civil liberties advocates that the FBI would *not* delete private financial or other information about Americans gathered under the broadened rules for issuing National Security Letters even if the person was cleared or the case was closed under the theory that the information might some day be relevant. In my view, this is an unacceptably intrusive and privacy damaging “standard.” It destroys the long-standing idea that criminal or intelligence agencies should not be keeping files or information on Americans without predication that they are doing something wrong. The FBI General Counsel also asserted that retaining personal private information on Americans who were cleared of any wrongdoing would be civil liberties-protective by making it easier to clear such persons again if their name came up later. While the “mosaic” theory may be a “precept” for gathering information about people abroad who are not extended certain protections guaranteed to people within the U.S., it is an utterly inappropriate policy for the American government to deploy against the American people. Intelligence gathering here must be properly focused in order to advance both the security *and* liberty of the American people, and that requires predication and judicial approval of such intrusions, in my view.

236. FISA Amendments Act of 2008, § 702, Pub. L. No. 110-261, 122 Stat. 2436 (to be codified in 50 U.S.C. § 1881a) (allowing the targeting of persons reasonably believed to be located outside the United States for the acquisition of foreign intelligence information, so long as the acquisition does not *intentionally* target any person *known at the time of acquisition* to be located in the United States).

237. Hayden distinguished between Americans’ “conversations” and “communications” being accessed by the NSA. See Hayden, *supra* note 241, at 7. (“This is not about intercepting *conversations* between people in the United States. This is not pursuit of *communications* entering or leaving America involving someone we believe is associated with al Qaeda. . . . When you’re talking to your daughter at state college, this program cannot intercept your *conversations*. And when she takes a semester abroad to complete her Arabic studies, this program will not intercept your *communications*.”) (emphasis added).

analyzed involve al Qaeda or foreign powers. And, once an American's call records, e-mail transactions, conversations, or written statements are intercepted in the broad pursuit of foreign intelligence information, there is no *statutory* requirement that a warrant be sought based on probable cause of wrongdoing such as conspiring to commit an act of violence.²³⁸

The bottom line is that the American people have no way to assess the effectiveness of such activities. American citizens do not know how much the NSA's budget is, although it has been reported to be eight billion dollars.²³⁹ The American people have not been informed about how much money is being spent to house the data that is now being accumulated on them, but there have been reports of several new buildings being built in the United States for storage and for analysis, and that technology is allowing data to become increasingly easy to store.²⁴⁰ The American people have been kept in the dark about how much is being spent to analyze American communications or conversations. And, the American people have no idea how much money the NSA or other agencies may be spending to buy access to third party records, data, or information about Americans.

We *do* know that the Executive Branch, at least in the prior Administration, has taken an expansive view of Supreme Court precedent about so-called third party records and argued that Americans have no cognizable privacy interest in keeping such records from the government. We also know that the Bush Administration engaged in "significant and systemic" "over-collection" of domestic communications of Americans, in a manner that went "beyond the broad legal limits established by Congress" in the 2008 FISA Amendment Act.

And there has been no clear explanation to the American people about how the government views the voluntary sharing of information with friends (or friends of friends) on Facebook or other social media. For example could a government agency, without disclosing its identity, create an "app" to obtain voluntary access to information? Or, could a private entrepreneur do so and then sell or share such information with the government? There are enormous risks to individual freedom in the current environment where the rules are unclear and every word spoken about these activities is so carefully selected to obscure the truth and protect both legitimate and illegitimate secrets. Once the government "normalizes" access to Americans' communications, we cannot control what future leaders may do with the newly accessible pool of information, even if the government currently has internal controls to "suppress" captured data or conversations that are not

238. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511 § 101(h), 92 Stat. 1783, 1785 (codified at 50 U.S.C. § 1801).

239. See Siobhan Gorman, *Budget Falling Short at NSA*, THE BALTIMORE SUN, January 17, 2007, http://articles.baltimoresun.com/2007-01-17/news/0701170100_1_alexander-budget-spy-agency (estimating the initial 2007 NSA budget to be approximately \$8 billion per year).

240. See BAMFORD, *supra* note 75, at 1, 3, 211.

operationally relevant—those data or conversations nonetheless remain available.

But, the American people have been denied an informed debate over how much this ill-advised focus on Americans and these broad collection efforts are costing us or how that money could be spent or might be better spent in ways that are more properly focused and that protect their legitimate privacy. As the House of Representatives noted in passing FISA, “While oversight can be, and the committee intends it to be, an important adjunct to control of intelligence activities, it cannot substitute for public laws, publicly debated and adopted, which specify under what circumstances and under what restrictions electronic surveillance for foreign intelligence purposes can be conducted.”²⁴¹ The American people need to understand more fully the risks of inviting the ears of the NSA onto these shores. That is not because the men and women of the NSA cannot be trusted, but because those in power, like Nixon and Bush/Cheney, will turn to them in manufactured (as with the claimed nuclear weapons purported to be in Iraq in 2002) or genuine crises and instruct them to do whatever is “technologically feasible.”

As Frank Church forewarned back in 1975, unless closely controlled, the powers of the NSA:

could be turned around on the American people, and no American would have any privacy left, such [is] the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide. If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back, because the most careful effort to combine together in resistance to the government, no matter how privately it is done, is within the reach of the government to know. Such is the capacity of this technology.²⁴²

That was the “abyss” Chairman Church feared. Turning the NSA’s technological weapons on the United States was the “bridge” he did not want to see us cross. But now, after the P.R. and lobbying campaign of President Bush’s Director of National Intelligence describing how essential it was to “modernize” FISA because of the advent of the Internet (shifting the rationale from the need to change the laws that were broken), we have crossed that bridge.

Fortunately, we have not fallen into the abyss. Yet, the technological capacity of the NSA of 1975 that Senator Church feared has been dwarfed by the NSA’s technological capacity and access today. And, now, that technological capacity has been turned inward, with internal “controls” that could be easily changed at the secret directives of those in charge. Unless we

241. H. REP. NO. 95-1283, at 21-22 (1978).

242. BAMFORD, *supra* note 75.

reconfirm privacy's status as an essential right, and police robust standards for its protection, no less than Americans' inalienable right to privacy and to freedom of speech, freedom of conscience, freedom of association, and, of course, freedom from the uninvited ear of the government could be lost.

* * *



JAMAIL CENTER FOR LEGAL RESEARCH
TARLTON LAW LIBRARY
THE UNIVERSITY OF TEXAS SCHOOL OF LAW

The Tarlton Law Library Oral History Series features interviews with outstanding alumni and faculty of The University of Texas School of Law.

Oral History Series

- | | |
|---|--|
| No. 1 - <i>Joseph D. Jamail, Jr.</i> 2005. \$20 | No. 6 - <i>James DeAnda</i> 2006. \$20 |
| No. 2 - <i>Harry M. Reasoner</i> 2005. \$20 | No. 7 - <i>Russell J. Weintraub</i> 2007. \$20 |
| No. 3 - <i>Robert O. Dawson</i> 2006. \$20 | No. 8 - <i>Oscar H. Mauzy</i> 2007. \$20 |
| No. 4 - <i>J. Leon Lebowitz</i> 2006. \$20 | No. 9 - <i>Roy M. Mersky</i> 2008. \$25 |
| No. 5 - <i>Hans W. Baade</i> 2006. \$20 | |

Forthcoming:

Gloria Bradford, Patrick Hazel, James W. McCartney,
Michael Sharlot, Ernest E. Smith, John F. Sutton, Jr.

*Other Oral Histories Published by the
Jamail Center for Legal Research*

- Robert W. Calvert* (Texas Supreme Court Trilogy, Vol. 1). 1998. \$20
Joe R. Greenhill, Sr. (Texas Supreme Court Trilogy, Vol. 2). 1998. \$20
Gus M. Hodges (Tarlton Law Library Legal History Series, No. 3). 2002. \$20
Corwin Johnson (Tarlton Law Library Legal History Series, No. 4). 2003. \$20
W. Page Keeton (Tarlton Legal Bibliography Series, No. 36). 1992. \$25
Jack Pope (Texas Supreme Court Trilogy, Vol. 3). 1998. \$20

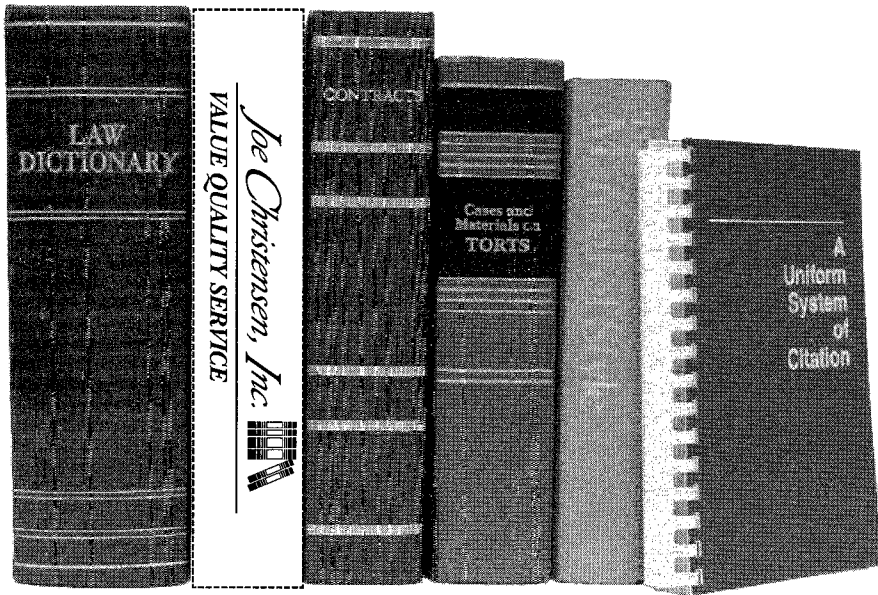
Order online at <http://tarlton.law.utexas.edu/> click on Publications
or contact Publications Coordinator,
Tarlton Law Library, UT School of Law,
727 E. Dean Keeton St., Austin, TX 78705
phone (512) 471-6228; *fax* (512) 471-0243;
email tarltonbooks@law.utexas.edu

THE UNIVERSITY OF TEXAS SCHOOL OF LAW PUBLICATIONS
What the students print here changes the world

Journal	domestic/foreign
Texas Law Review http://www.texaslawreview.org	\$47.00 / \$55.00
Texas International Law Journal http://www.tilj.org	\$35.00 / \$40.00
Texas Environmental Law Journal http://www.texenrls.org/publications_journal.cfm	\$40.00 / \$50.00
American Journal of Criminal Law http://www.ajcl.org	\$30.00 / \$35.00
The Review of Litigation http://www.thereviewoflitigation.org	\$30.00 / \$35.00
Texas Journal of Women and the Law http://www.tjwl.org	\$30.00 / \$35.00 individuals \$40.00 / \$45.00 institutions
Texas Intellectual Property Law Journal http://www.tiplj.org	\$25.00 / \$30.00
Texas Hispanic Journal of Law & Policy http://www.thjlp.org	\$30.00 / \$40.00
Texas Journal On Civil Liberties & Civil Rights http://www.txjclcr.org	\$40.00 / \$50.00
Texas Review of Law & Politics http://www.trolp.org	\$30.00 / \$35.00
Texas Review of Entertainment & Sports Law http://www.tresl.net	\$40.00 / \$45.00
Texas Journal of Oil, Gas & Energy Law http://www.tjogel.org	\$30.00 / \$40.00
Manuals:	
<i>Texas Rules of Form</i> 11th ed. ISBN 1-878674-07-2	
<i>Manual on Usage & Style</i> 11th ed. ISBN 1-878674-55-2	

To order, please contact:
The University of Texas School of Law Publications
727 E. Dean Keeton St.
Austin, TX 78705 U.S.A.
Publications@law.utexas.edu


ORDER ONLINE AT:
<http://www.texaslawpublications.com>



We Complete the Picture.

In 1932, Joe Christensen founded a company based on Value, Quality and Service. With 77 years of printing experience, Joe Christensen, Inc. remains the most experienced Law Review printer in the country.

Our printing services bridge the gap between your editorial skills and the production of a high-quality publication. We ease the demands of your assignment by offering you the basis of our business—customer service.

Joe Christensen, Inc. 

1540 Adams Street
Lincoln, Nebraska 68521-1819
Phone: 1-800-228-5030
FAX: 402-476-3094
email: sales@christensen.com

Value

Quality

Service

Your Service Specialists

Texas Law Review

Texas Rules of Form

Eleventh Edition

The updated guide includes the new citation form for Texas Supreme Court petition history.

Texas Law Review Manual on Usage & Style

Tenth Edition

A pocket reference guide on style for all legal writing.

School of Law Publications
University of Texas at Austin

727 East Dean Keeton Street

Austin, Texas 78705-3299

Fax: (512) 471-6988 Tel: (512) 232-1149

Order online: <http://www.texaslawpublications.com>

