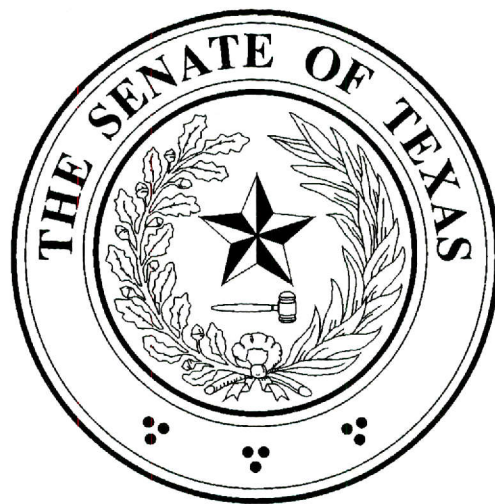


Senate Committee on State Affairs

Interim Report to the 84th Legislature



January 2015



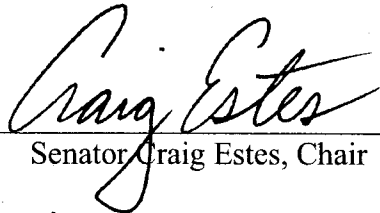
January 23, 2015

The Honorable David Dewhurst
Lieutenant Governor of Texas
Members of the Texas Senate
Texas State Capitol
Austin, Texas 78701

Dear Lieutenant Governor Dewhurst and Fellow Members:

The Committee on State Affairs of the Eighty-Third Legislature hereby submits its interim report including findings and recommendations for consideration by the Eighty-Fourth Legislature.

Respectfully submitted,



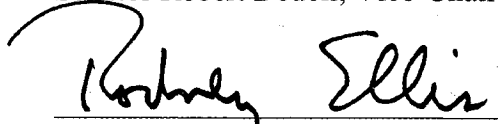
Senator Craig Estes, Chair



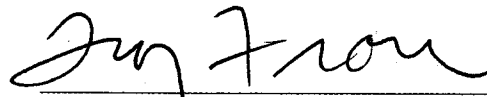
Senator Robert Deuell, Vice-Chair




Senator Brandon Creighton



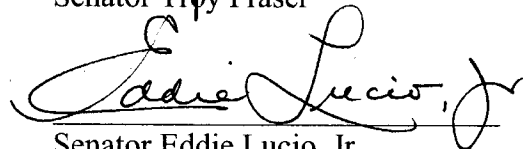
Senator Rodney Ellis



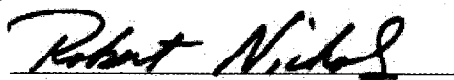
Senator Troy Fraser



Senator Joan Huffman



Senator Eddie Lucio, Jr.



Senator Robert Nichols

Senator Leticia Van de Putte



TABLE OF CONTENTS

INTERIM CHARGES	i
SENATE COMMITTEE ON STATE AFFAIRS INTERIM HEARINGS	iii
INTERIM CHARGE DISCUSSIONS AND RECOMMENDATIONS	1
CHARGE NO. 1	1
BACKGROUND	1
<i>Patent Law Basics</i>	1
<i>The "Patent Troll" Controversy</i>	1
<i>Effect on Innovation</i>	3
DISCUSSION	4
<i>Enforcement of Patents Governed by Federal Law</i>	4
<i>What Other States Are Doing</i>	4
<i>Potential State-Law Solutions</i>	6
RECOMMENDATION	8
CHARGE NO. 2	9
ANY NECESSARY LIMITS ON WARRANTLESS SEARCH AND SEIZURE OF DATA FROM ELECTRONIC DEVICES AND WIRELESS PROVIDERS, INCLUDING DIGITAL CONTENT AND GEOLOCATIONAL DATA	9
ANY NECESSARY PROTECTIONS AGAINST NON-CONSENTED VIDEO AND AUDIO RECORDINGS COLLECTED BY PRIVATE HANDHELD AND WEARABLE MOBILE DEVICES AND OTHER PRIVATE SURVEILLANCE.	20
NECESSARY LIMITS ON WARRANTLESS MONITORING OF THE PHYSICAL LOCATION OF INDIVIDUALS THROUGH THE USE OF BIOMETRICS, RFID CHIPS, FACIAL RECOGNITION, OR OTHER TECHNOLOGIES.....	26
RECOMMENDATION	36
CHARGE NO. 3	36
WHETHER SUFFICIENT PROTECTIONS EXIST FOR DNA SAMPLES AND INFORMATION, INCLUDING WHETHER THERE SHOULD BE A PROHIBITION ON THE CREATION OF DNA DATABASES, EXCEPT FOR FELONS AND SEX OFFENDERS.	36
MECHANISMS TO ENSURE THAT PRIVATE HEALTH CARE INFORMATION IS PROPERLY PROTECTED.	45
WAYS TO ENSURE THAT PREVIOUSLY ANONYMOUS DATA IS NOT IMPROPERLY RE-IDENTIFIED AND MARKETED.	52
RECOMMENDATION	57
CHARGE NO. 4	57
RECOMMENDATION	60
CHARGE NO. 5	61
INTERACTIVE FORUMS	61

OTHER INITIATIVES: RECENT DEVELOPMENTS ON THE TEXAS SENATE WEBSITE	62
RECOMMENDATION	63
CHARGE NO. 6.....	63
BACKGROUND	63
TEXAS HEALTH INSURANCE POOL.....	64
NAVIGATORS.....	65
THE ACA ROLLOUT IN TEXAS.....	66
<i>Premium Increases</i>	66
<i>Texas Enrollment</i>	68
<i>Effect on Texas Employers</i>	71
<i>Provider Challenges</i>	73
FREE MARKET ALTERNATIVES: SELF-INSURANCE	75
RECOMMENDATION.....	75
CHARGE NO. 7.....	76
MEDICAL PRICE TRANSPARENCY	76
<i>Healthcare Literacy</i>	77
<i>Transparency Framework</i>	77
SENATE BILL 1731, 80TH LEGISLATURE.....	78
<i>Texas Department of Insurance</i>	79
TRANSPARENCY AND THE BALANCE BILLING PROBLEM	81
<i>Transparency and Emergency Room Billing</i>	82
<i>Transparency and Balance Billing Outside the Emergency Room Context</i>	82
<i>Is Transparency Enough</i>	83
RECOMMENDATION	83
CHARGE NO. 8.....	83
ACTUARIAL AND FINANCIAL CONDITIONS OF THE PENSION AND HEALTH CARE	
PROGRAMS	83
RECOMMENDATION.....	88
CHARGE NO. 9.....	88
CHARGE NO. 10	89
BACKGROUND	89
HEARING	89
RECOMMENDATION	89

Interim Charges

The Senate State Affairs Committee is charged with conducting a thorough and detailed study of the following issues, including state and federal requirements, and preparing recommendations to address problems or issues that are identified.

1. Examine the negative economic impact on Texas business from legal issues involving threatened and actual patent litigation by "patent assertion entities" (PAEs). Consider the effects of PAE actions on innovation and economic development in Texas, paying particular attention to threats and lawsuits involving software and technology patent claims. Make recommendations on how the State of Texas can address problems related to frivolous legal actions and unsubstantiated patent claims asserted against legitimate business enterprises in light of the relevant federal jurisdiction, laws, regulations, and court rules in patent cases.
2. Examine possible measures to protect the personal privacy of Texas residents from governmental and commercial surveillance, including: (1) any necessary limits on warrantless search and seizure of data from electronic devices and wireless providers, including digital content and geolocational data; (2) any necessary protections against non-consented video and audio recordings collected by private handheld and wearable mobile devices and other private surveillance; and (3) any necessary limits on warrantless monitoring of the physical location of individuals through the use of biometrics, RFID chips, facial recognition, or other technologies. Examine related measures proposed or passed in other states.
3. Review the types and scope of personal data collected by governmental and commercial entities and consider methods to minimize the government's collection of data on its citizens. The study should include: (1) whether sufficient protections exist for DNA samples and information, including whether there should be a prohibition on the creation of DNA databases, except for felons and sex offenders; (2) methods to protect the privacy of gun owners from aggregated purchasing pattern tracking; (3) mechanisms to ensure that private health care information is properly protected; and (4) ways to ensure that previously anonymous data is not improperly re-identified and marketed. Examine related measures proposed or passed in other states.
4. Examine possible reforms designed to increase citizens' ability to know what data is being collected about them by governmental and commercial entities and with whom that data is being shared, including an analysis of consumer informed consent. Examine related measures proposed or passed in other states.
5. Study the online legislative resources available to the public from Texas Senate Committee websites and compare resources to those provided by other state legislative committees in Texas and other states. Determine how Texas Senate websites can be improved to provide a more interactive and transparent government.

6. Study the emerging negative impacts of the Federal Affordable Care Act, including the use of navigators, and make recommendations to mitigate any unintended consequences including rising health insurance premiums, lack of access to healthcare, mishandling of Texans' private information by insufficiently-trained navigators, and the Act's overall effect on Texas employers and insurance consumers. Evaluate free-market alternatives to the Act, including state-led proposals to repeal, reduce or replace the Act. Closely monitor and make recommendations on the continuation of the Texas Health Insurance Pool.
7. Study and make recommendations on increasing medical price transparency in Texas, including studying the impact of Senate Bill 1731, 80th Legislative Session. Analyze relevant reforms considered or implemented in other states, and make recommendations regarding potential changes designed to create a more open marketplace for enhanced consumer decision making in Texas.
8. Monitor the actuarial and financial conditions of the pension and health care programs administered by the Teacher Retirement System (TRS) and the Employees Retirement System (ERS).
9. Monitor the implementation of legislation addressed by the Senate Committee on State Affairs, 83rd Legislature, Regular Session, and make recommendations for any legislation needed to improve, enhance, and/or complete implementation.
10. Study and make recommendations relative to the structure of Texas Mutual Insurance Company and the residual market for workers' compensation insurance in Texas.

Senate Committee on State Affairs Interim Hearings

September 15, 2014, Capitol Extension Rm. E1.012

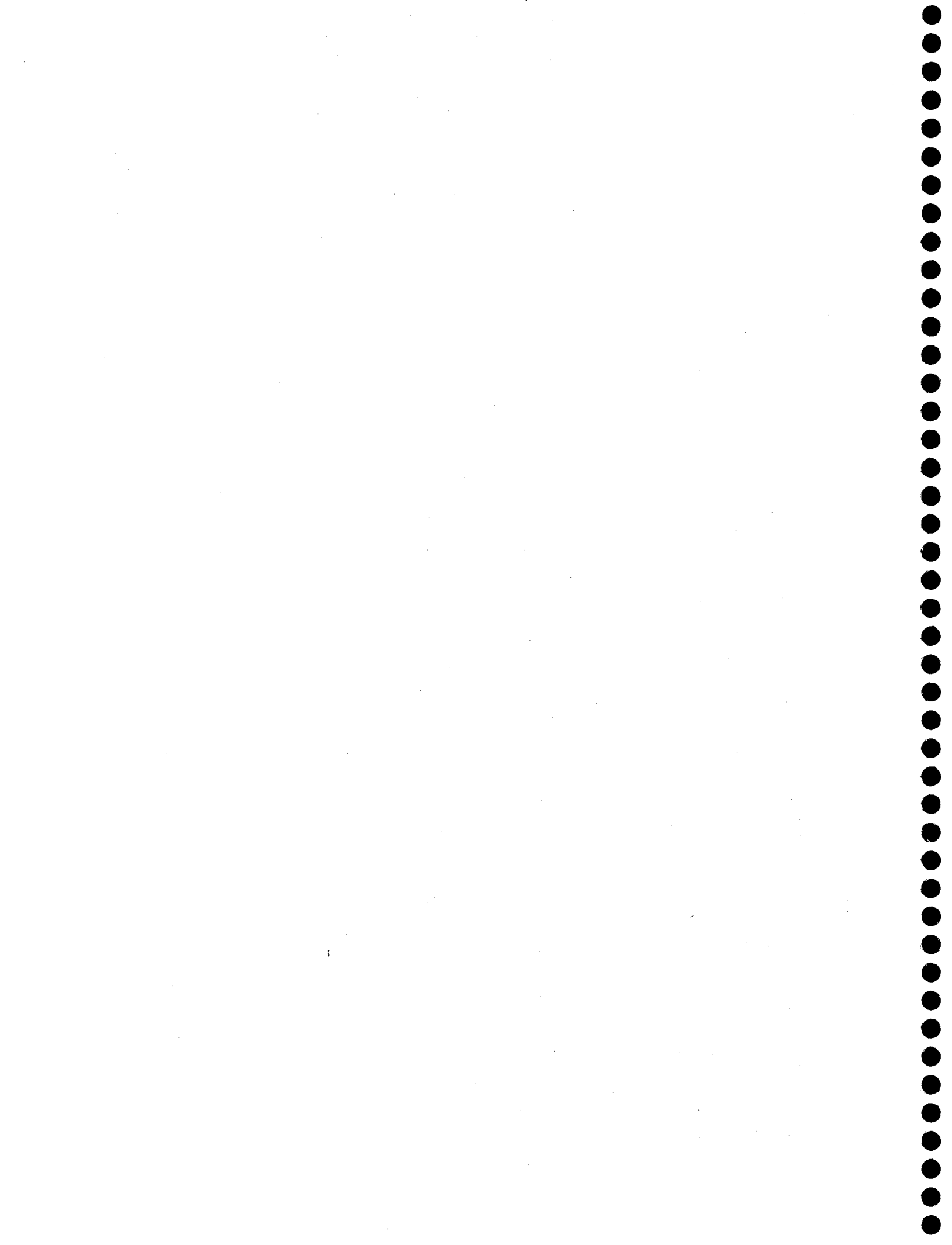
The Committee took invited testimony on Charge Nos. 1, 6, 7 and 10.

September 16, 2014, Capitol Extension Rm. E1.012

The Committee took invited testimony on Charge Nos. 2, 3, 4 and 5.

December 9, 2014, Betty King Rm. 2E.20

The Committee took invited testimony on Charge No. 8.



Interim Charge Discussion and Recommendations

Charge No. 1

Examine the negative economic impact on Texas business from legal issues involving threatened and actual patent litigation by "patent assertion entities" (PAEs). Consider the effects of PAE actions on innovation and economic development in Texas, paying particular attention to threats and lawsuits involving software and technology patent claims. Make recommendations on how the State of Texas can address problems related to frivolous legal actions and unsubstantiated patent claims asserted against legitimate business enterprises in light of the relevant federal jurisdiction, laws, regulations, and court rules in patent cases.

Background

Patent Law Basics

A strong intellectual property system supports and enables the innovation that is the lifeblood of our economy. Our patent system is enshrined in our Constitution to encourage invention and to reward Americans for their hard work and risk-taking.

The constitutional foundation of federal patent law is found in Article I, Section 8, Clause 8 of the United States Constitution, which gives Congress the power "[t]o Promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."¹ Patent law also has a statutory basis in the Patent Act of 1952.² Patents are acquired by submitting an application to the U.S. Patent Trademark Office, and if granted, patents provide the right to exclude others from making, selling, using, or importing a claimed invention for a period of time.

Disputes over patent ownership and rights are within the exclusive jurisdiction of federal courts. A patent holder may enforce its rights by filing a patent infringement suit in federal court against anyone who makes, uses, sells, or imports the patented technology, whether or not it was copied or developed independently. Patent infringement suits can be very expensive. According to a survey by the American Intellectual Property Law Association, an average suit with \$1 million to \$25 million at stake costs \$1.6 million through discovery and \$2.8 million through trial.³

The "Patent Troll" Controversy

In recent years, the patent system has seen the growth of abusive patent litigation designed not to reward innovation but to threaten inventors and companies based on questionable claims. Patent assertion entities (PAEs), also known as "patent trolls," are individuals or companies that capitalize on their patents solely through licensing and litigation. The PAE business model focuses on buying and asserting patents rather than on developing or commercializing patented

¹ U.S. CONST. art. I, §8, cl. 8.

² P.L. 82-593, 66 Stat. 792 (codified at 35 U.S.C.).

³ AMERICAN INTELLECTUAL PROPERTY LAW ASSOCIATION, 2011 REPORT OF THE ECONOMIC SURVEY (2012).

inventions.⁴ Certain PAEs seek and obtain broad and vague patents, with the intent of suing other companies for illegally infringing on those patents. These PAEs hope that companies will pay to avoid costly litigation. Sometimes PAEs create shell companies that make it difficult for businesses to know who is threatening to sue them. They identify potential infringers of those patents, and send demand letters offering those alleged infringers licensing of the patent or settlement of threatened litigation.⁵ However, it should be recognized that while PAEs often do not commercialize the patents, they reward the inventor's intellectual work by purchasing his or her patent, and thus fulfill the purpose of patents, which is to incentivize people to engage in research and development.

PAEs differ greatly from traditional non-practicing entities (NPEs) that own patents but do not make products with them, and yet play an important role in innovation by connecting manufacturers with inventors.⁶ Traditional NPEs, such as universities, research entities, and design firms, act as intermediaries that reduce transaction costs between those who invent things and those who develop and commercialize them.⁷ Unlike traditional NPEs, however, PAEs focus on aggressive litigation tactics, such as threatening to sue companies without specific evidence of infringement and asserting their patents cover inventions not imagined at the time the patents were granted.⁸

Historically, PAEs have targeted the big online players like Google and Yahoo. More recently, however, they have gone after small businesses, restaurants, non-profits, and small financial institutions, which are attractive targets because they generally lack the recourses to defend a lengthy lawsuit. According to a White House report, one PAE sent 8,000 demand letters to coffee chains, hotels, and retailers seeking compensation for offering Wi-Fi to customers.⁹

The White House estimates that lawsuits brought by PAEs dramatically increased in the last two years, rising from twenty-nine percent of all patent suits to sixty-two percent of all patent suits.¹⁰ A plurality of these new cases were filed in the Eastern District of Texas.¹¹ The Eastern district of Texas ranked number one in districts with the most new cases filed in 2013.¹² In a separate study, Boston University researchers estimated that in 2011, more than 2,100 companies were forced to mount 5,842 defenses in lawsuits from PAEs, up from 1,401 lawsuits in 2005, at a cost

⁴ BRIAN T. YEH, CONGRESSIONAL RESEARCH SERVICE, AN OVERVIEW OF THE "PATENT TROLLS" DEBATE I (2013), available at <http://www.fas.org/sgp/crs/misc/R42668.pdf>.

⁵ Ahmed J. Davis and Karolina Jesien, *The Balance of Power in Patent Law: Moving Towards Effectiveness in Addressing Patent Troll Concerns*, 22 *Fordham Intell. Prop. Media & Ent. L.J.* 835, 836 (2012).

⁶ EXEC. OFFICE OF THE PRESIDENT, PATENT ASSERTION AND U.S. INNOVATION (2013), available at http://www.whitehouse.gov/sites/default/files/docs/patent_report.pdf [hereinafter U.S. Innovation].

⁷ Steven M. Cherry, *Patent Profiteers*, *IEEE SPECTRUM*, June 2004, at 38-41.

⁸ U.S. Innovation, *supra* note 7.

⁹ *Id.*

¹⁰ *Id.*

¹¹ OWEN BYRD & BRIAN HOWARD, LEX MACHINA, 2013 PATENT LITIGATION YEAR IN REVIEW (2013), available at https://fortunedotcom.files.wordpress.com/2014/05/lexmachina-2013_patent_litigation_year_in_review.pdf?aliId=337013.

¹² *Id.*

of \$29 billion.¹³ A recent report, however, shows PAEs lose ninety-two percent of judgments for lack of merit.¹⁴ Despite these odds, few cases actually make it to trial, because the vast majority of defendants settle regardless of the merits due to the fact that litigation is risky, disruptive, and expensive.¹⁵ In order to continue operations, recipients of PAE letters typically pay licensing fees, which are strategically set well below litigation costs.¹⁶

Effect on Innovation

The patent system is intended to protect and encourage innovation. Recent studies indicate that currently PAEs do more harm than good to innovation and the patent system.¹⁷ For example, investment decisions must factor in the likelihood that PAEs will later emerge and demand royalties or bring costly litigation, which will directly reduce returns on investment.¹⁸ Businesses and startups may have a difficult time getting funding from venture capitalists and other investors who anticipate future PAE demands.

There are also opportunity costs as entities that commercialize their patents divert funds from research and development to handle PAE demands. Not only is there the obvious diversion to pay licensing fees and legal costs, but there has also been increased investment in PAEs instead of startups or other businesses. Some investors buy stakes in PAEs to hedge against the risk of being sued, while others believe PAEs offer better returns on investment than most startups and shift funding in that direction.¹⁹

On the other hand, PAEs argue they actually promote investment in invention. The most recognized benefit of PAE activity is increased liquidity and better risk management for investments applied to research and invention. Universities, for example, routinely obtain and sell patents in the secondary market and benefit directly from PAE activity and never bear the costs of licensing fees and litigation.²⁰ The more licensing fees PAEs obtain, the more these inventors earn from their patents and the greater their incentives to invent.

Invention, however, is only the first step in a lengthy and expensive development process to bring innovation to the market. Although PAEs may aid in increasing the volume of invention, they may create disincentives for firms to invest in the rest of the process required to bring

¹³ James Bessen, Jennifer Ford, & Michael J. Meurer, *The Private and Social Costs of Patent Trolls* (Boston University School of Law Working Paper No. 11-45 (September 19, 2011), available at <http://www.bu.edu/law/faculty/scholarship/workingpapers/2001.html>).

¹⁴ John R. Allison, Mark A. Lemley & Joshua Walker, *Patent Quality and Settlement Among Repeat Patent Litigants*, 99 GEO. L.J. 677, 694 (2011).

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ FEDERAL TRADE COMMISSION, *THE EVOLVING IP MARKETPLACE: ALIGNING PATENT NOTICE AND REMEDIES WITH COMPETITION* at 40 n. 43 (2011).

¹⁸ *Id.*

¹⁹ *Abusive Patent Litigation: The Impact on American Innovation & Jobs, and Potential Solutions: Hearing Before the H. Subcomm. on Courts, Intellectual Prop. and the Internet*, 113th Cong. (2013).

²⁰ Mark A. Lemley, *Are Universities Patent Trolls?*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 611, 618 (2008).

inventions to the market. In fact, the more a firm invests in research and development, the more likely it is to be sued by a PAE.²¹

Discussion

Enforcement of Patents Governed by Federal Law

As previously mentioned, patent disputes are within the exclusive jurisdiction of federal courts. Federal law may preempt related state regulation to the extent the state law poses "an obstacle to the accomplishment and execution of the full purpose and objectives of Congress."²² Courts regularly use the federal preemption doctrine to strike down state laws that conflict with the federal patent laws or the policies contained in those federal laws. In *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, for example, the United States Supreme Court stated that its "past decisions have made clear the state regulation of intellectual property must yield to the extent that it clashes with the balance struck by Congress in our patent laws."²³ Under this general preemption standard, the United States Court of Appeals for the Federal Circuit in *Zenith Elecs. Corp. v. Exzec., Inc.* held that a person who asserts patent rights in good faith may not be made subject to state tort liability because the state action is preempted by federal patent law.²⁴ In *Globetrotter Software, Inc. v. Elan Computer Group, Inc.*, the federal circuit court reaffirmed its decision in *Zenith* by holding that state law claims against a person asserting patent infringement in pre-litigation communications can survive federal preemption only to the extent those claims are based on a showing of "bad faith" in asserting the claim.²⁵

Under these cases state tort law may provide for liability for the assertion of patent rights in communications warning about potential litigation, but only if there is a showing that those assertions are made in bad faith. Applying the bad faith doctrine, the federal circuit court in *Globetrotter* held that only "objectively baseless allegations of infringement" can give rise to state tort liability.²⁶ To satisfy *Globetrotter's* "objectively baseless" standard, it must be proved that "no reasonable litigant could realistically expect success on the merits."²⁷

What Other States Are Doing

State Attorneys General in Minnesota, New York, and Vermont have taken actions to rein in PAEs. Additionally, earlier this year, the National Association of Attorneys General sent a letter to the Chairmen of the Senate Judiciary and Commerce, Science and Transportation Committees supporting efforts to enact bipartisan patent reform legislation. One of the reasons cited in the

²¹ Colleen V. Chien, *Of Trolls, Davids, Goliaths, and Kings: Narratives and Evidence in the Litigation of High-Tech Patents*, 87 N.C.L. REV. 1571, 1581 (2009).

²² See, e.g., *Hines v. Davidowitz*, 312 U.S. 52, 67 (1941).

²³ 489 U.S. 141, 152 (1989).

²⁴ 182 F.3d 1340, 1355 (Fed. Cir. 1999).

²⁵ 362 F.3d 1367, 1374 (Fed. Cir. 2004) "[B]ad faith must be alleged and ultimately proven, even if bad faith is not otherwise an element of the tort claim." (quoting *Zenith*, 182 F.3d at 1355).

²⁶ 362 F.3d at 1377 ("[F]ederal patent laws preempt state laws that impose tort liability for a patentholder's good faith conduct in communications asserting infringement of its patent and warning about potential litigation.").

²⁷ *Id.* at 1376 (quoting *Profl Real Estate Investors, Inc. v. Columbia Pictures Indus., Inc.*, 508 U.S. 49, 57 (1993)).

letter for their support is their belief that PAEs stifle innovation and harm our economy. General Abbott is a signatory of that letter.²⁸

Patent reform has come to a standstill in Congress, and as a result, states are taking action on their own to curb patent abuses. State-based legislation targets vaguely-worded demand letters and centers on the concept that "bad faith" assertions of patents violate existing consumer protection laws. This model was first adopted by the Vermont legislature in 2013. A total of 27 states have considered such legislation, and to date, eighteen of these states have adopted anti-patent-troll laws. Below is a map that shows which states have enacted or are considering state-based legislation.

Demand Letter Legislation in the States as of 8/28/2014



Source: PatentProgress.org

²⁸ See Appendix to Charge 1.

This new wave of legislation will give states some authority over PAEs that use demand letters as a key part of their strategy. In general, the state bills allow state courts to consider a variety of factors in deciding what a "bad faith" assertion is. Patent owners who fail to disclose the ownership of their patents, or show that they have not investigated the target's alleged infringement at all, are more likely to be considered to be using their patents in "bad faith." However, states alter the Federal Rules of Civil Procedure, which are primarily at fault in making it difficult for courts to dismiss questionable cases quickly before large amounts of resources have been expended. Meaningful reform that addresses this problem will have to come from the federal level.

Potential State-Law Solutions

Potential Use of State Consumer Protection Laws

Several states have sought to address patent abuse using state consumer protection laws prohibiting bad faith clams. *Zenith* and *Globetrotter* involved parties attempting to obtain relief against patent holders for alleged bad faith conduct by applying existing state laws prohibiting unfair competition.²⁹ The Attorneys General of Vermont and Nebraska have taken action against PAEs under existing state consumer protection laws.³⁰

In Texas this would mean adding a bad faith claim of patent infringement to the Texas Deceptive Trade Practices Act (DTPA). Implementing this type of legislation in Texas, however, is not so cut and dry. If the legislature expands the DTPA to add a bad faith claim for patent infringement, the legislature would also have to expand the definition of consumer. Currently, the term does not include a business consumer that has assets of \$25 million or more, or that is owned or controlled by a corporation or entity with assets of \$25 million or more.³¹ In order to capture both large and small businesses impacted by PAEs, we would need to broaden this definition.

Private Cause and Attorney General Cause of Action

Vermont enacted the first state law to specifically address the patent abuses by PAEs.³² The Vermont statute creates a private cause of action and an Attorney General cause of action for bad faith claims of patent infringement. Specifically, the legislation prohibits a person from making "a bad faith assertion of patent infringement" and creates a cause of action known as a "threats action," where the recipient of a legal threat can bring against a person who wrongfully asserts legal rights.³³ The statute creates a cause of action based on pre-litigation conduct, in contrast to more common tort reform measures, which affect lawsuits that have already been filed.

In the absence of a definite decision by the United States Supreme Court regarding federal preemption of state regulation in this particular area, legal scholars disagree as to whether the Vermont bill and other similar state legislative efforts can avoid federal preemption. Some argue

²⁹ See *Zenith* 182 F.3d at 1355; *Globetrotter* 362 F.3d at 1374.

³⁰ See *Vermont and Nebraska Attorneys General Take Patent Trolls Head On*, NAA Gazette, <http://www.naag.org/vermont-and-nebraska-attorneys-general-take-patent-trolls-head-on.php>.

³¹ Texas Bus. & Com. Code Ann. § 17.45(4).

³² See Eric Goldman, *Vermont Enacts the Nation's First Anti-patent Trolling Law*, *Forbes* (May 22, 2013), <http://www.forbes.com/sites/ericgoldman/2013/05/22/vermont-enacts-the-nations-first-anti-patent-trolling-law>.

³³ Vt. Stat. Ann. tit. 9, § 4197 (West 2013).

these state efforts are themselves preempted because they ultimately interfere with the federal government's exclusive power to regulate patent claims.³⁴ Other scholars disagree, arguing that the Vermont Statute will withstand federal preemption scrutiny because it has been carefully drafted to comply with the federal circuit court's "objectively baseless" standard for determining whether a patent assertion has been made in bad faith.³⁵

While this type of state legislation has not been tested in the United States Supreme Court, Vermont's Attorney General recently brought a suit against an alleged "patent troll" under the state's bad faith legislation. The defendant PAE tried to remove the suit to federal court under subject matter jurisdiction, but the United States Court of Appeals for the Federal Circuit referred the suit back to Vermont state court.³⁶ This is the first known patent trolling lawsuit to be filed on the basis of traditional consumer protection laws and this ruling is the first step towards resolving the preemption debate.

Many businesses argue that a private cause of action threaten valid patent holders, chilling the exercise of their rights, and might not be effective in curbing abusive behavior.³⁷ A private cause of action could incentivize abusive litigation against patent owners. As an alternative to a private cause of action, these businesses suggest that the Attorney General serve as a repository for complaints regarding suspected "bad-faith demand" letters. However, creating a new Attorney General cause of action expands government power over individuals, increases state spending, and burdens the agency.

Improving Notice

Improving notice and the information contained in the demand letters is a high-priority goal of some patent reform advocates. Many scholars believe solving this notice failure would go far towards reducing the negative effects of PAEs while keeping the benefits and making the entire patent system work better. Under this approach, states have thus far been able to require that demand letters contain certain information, such as a patent number identifying the patent that is allegedly being infringed upon; material information so an accused infringer can evaluate the claim; a clear explanation for the factual basis for its proposed fee; and transparency of the true identity of the patent holder. However, Texas may be preempted from targeting demand letters in this way by federal law, as state law cannot add requirements for filing a lawsuit in federal court.

Establishing requirements for demand letters is not without critics. Some argue that, as a policy matter, it is undesirable to have states regulating intellectual property issues and what notice is required.³⁸ State laws create a patchwork approach that interferes with a more unified federal regulation. Some businesses are concerned that state legislation regarding demand letters would

³⁴ See Eric Goldman, *Vermont Enacts the Nation's First Anti-patent Trolling Law*, *Forbes* (May 22, 2013), <http://www.forbes.com/sites/ericgoldman/2013/05/22/vermont-enacts-the-nations-first-anti-patent-trolling-law>.

³⁵ See Camilla A. Hardy, *What Is Happening in Vermont? Patent Reform From the Bottom Up* (May 27, 2013), <http://patentlyo.com/patent/2013/05/what-is-happening-in-vermont-patent-law-reform-from-the-bottom-up.html>.

³⁶ *Vermont v. MPHJ Tech. Inv., LLC*, No. 2014-137 (Fed. Cir. Aug. 11, 2014).

³⁷ See Appendix to Charge 1.

³⁸ Eric Goldman, *supra* note 34 (arguing that "it would be troublesome if states adopt inconsistent or different legal standards for threats actions; it becomes exponentially more expensive for IP owners to enforce their rights when they have to research and comply with multitudinous state laws").

interfere with legal business-to-business communication and inadvertently chill legitimate patent communications.

Demand Letter Registry

Another solution to the PAE issue is to create a public registry of "patent troll" demand letters. The idea behind this solution is that transparency would help curb the unwarranted and costly attacks businesses and their customers face from the PAEs. This approach would create a publicly accessible database for patent infringement claims for claimants that send a specified number of demand letters a year. This requires registration with the secretary of state, disclosure of affiliates, copies of demand letters sent to anyone in the U.S., and a registration fee. The legislation also creates a Target Demand Letter Database allowing targets of demand letters to provide the secretary of state copies of demand letters and other relevant information. This database will be accessible by targets that receive the same demand letters.

This approach, however, has many critics. Companies must be able to protect their patents and engage in legitimate business-to-business communication.³⁹ If a business believes a competitor's design will infringe on a patent, the business will send a notice letter, which encourages communication and helps avoid litigation. It is important that demand letter registry legislation set the number of demand letters required to trigger registration at a number low enough to target true PAEs, but high enough to avoid also encompassing legitimate patent claims.

Recommendation

Although there is clearly an issue with abuse of the patent system, the solutions are complex. The Committee recommends that the Legislature continue to study the issue and monitor the states that have enacted such laws.

It is unclear what state action would be effective in curbing the potential abuses of patent enforcement. Disputes over patent ownership and rights are within the exclusive jurisdiction of federal courts. Federal courts regularly use the federal preemption doctrine to strike down state laws that conflict with federal patent laws and the policies contained in those federal laws. However, a showing that a person seeking to enforce a patent does so in bad faith may bring conduct relating to patent enforcement into the realm of state regulation.

States do not have the power to directly fix the federal patent system, but states can look to ways to regulate, restrict, and discourage the behavior of excessive bad faith demand letters. However, because state solutions are relatively new and novel, the federal courts have yet to rule on the inevitable federal preemption issue. While the Legislature could consider enacting its own version of a statute to address patent trolling, it is impossible to predict with certainty whether such a statute would be both effective in curbing allegedly abusive "patent trolling" activities and constitutional under the preemption doctrine.

Aside from the preemption issue, legislation should be limited to those who send false and misleading demand letters sent in bad faith to large populations of end users to extort settlements, routine business-to-business communication should not be swept-in.

³⁹ Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Kathy Barber, Caterpillar, Inc.).

Charge No. 2

Examine possible measures to protect the personal privacy of Texas residents from governmental and commercial surveillance, including: (1) any necessary limits on warrantless search and seizure of data from electronic devices and wireless providers, including digital content and geolocation data; (2) any necessary protections against non-consented video and audio recordings collected by private handheld and wearable mobile devices and other private surveillance; and (3) any necessary limits on warrantless monitoring of the physical location of individuals through the use of biometrics, RFID chips, facial recognition, or other technologies. Examine related measures proposed or passed in other states.

Any necessary limits on warrantless search and seizure of data from electronic devices and wireless providers, including digital content and geolocation data.

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.

- Fourth Amendment to the United States Constitution

The people shall be secure in their persons, houses, papers and possessions, from all unreasonable seizures or searches, and no warrant to search any place, or to seize any person or thing, shall issue without describing them as near as may be, nor without probable cause, supported by oath or affirmation.

- Article 1, Section 9 of the Texas Constitution

The Fourth Amendment to the United States Constitution and Art. 1 Sec. 9 of the Texas Constitution protect "persons, houses, papers, and effects" from unreasonable government searches.⁴⁰ ⁴¹ Generally, a search is unreasonable if not authorized by a valid warrant.⁴² A valid warrant requires probable cause, particularity, and the affirmation of a neutral magistrate. To demonstrate probable cause and particularity the government must present facts and circumstances based on reasonably trustworthy information that are sufficient to warrant a reasonable person to believe a particular person, place, or property is involved in or evidence of a criminal offense that has been or is presently being committed.⁴³ ⁴⁴ However, not all warrantless searches are unreasonable. For example, a valid warrant is not required when a search is conducted under exigent circumstances.⁴⁵ Moreover, following a lawful arrest, the government may conduct a warrantless search for weapons or evidence of criminality incident to that arrest.⁴⁶

⁴⁰ U.S. CONST. amend. IV.

⁴¹ T.X. Const. art. I, § 9.

⁴² California v. Carney, 471 U. S. 386, 390-391 (1985).

⁴³ Carroll v. United States, 267 U.S. 132, 162 (1925).

⁴⁴ Marron v. United States, 275 U.S. 192, 196 (1927).

⁴⁵ Mincey v. Arizona, 437 U.S. 385 (1978).

⁴⁶ Agnello v. United States, 269 U.S. 20, 30 (1925).

Additionally, the government may search a vehicle without a valid warrant, if there is probable cause to believe the vehicle contains evidence of a crime.⁴⁷

The Supreme Court has repeatedly held that a "search" under the Fourth Amendment only takes place when the government intrudes upon or invades a place where a person has a reasonable expectation of privacy.⁴⁸ ⁴⁹ For example, a person has a reasonable expectation of privacy from government intrusion in his or her body,⁵⁰ home,⁵¹ hotel room,⁵² and mail.⁵³ He or she does not, however, have a reasonable expectation of privacy in property or information "knowingly exposed to the public," or provided to third parties.⁵⁴ This is known as the Third Party Doctrine. According to that doctrine, the Fourth Amendment does not protect information voluntarily provided to third parties, such as banks⁵⁵ and phone companies,⁵⁶ because a person "has no legitimate expectation of privacy in information voluntarily turned over to a third party."⁵⁷

In response to the Third Party Doctrine and the growing use of electronic communications, such as e-mail, Congress passed the Stored Communications Act (SCA) as Title II of the Electronic Communications Privacy Act (ECPA) of 1986.⁵⁸ Section 2703 of the SCA establishes standards the government must meet to require disclosure of electronic communications by electronic communications service (ECS) providers and remote computing service (RCS) providers.⁵⁹ Under the SCA, compelling an ECS provider to disclose the content of an electronic communication held in electronic storage for less than 180 days requires a valid search warrant.⁶⁰ Furthermore, compelling an RCS provider to disclose the content of an electronic communication or forcing an ECS provider to disclose the content of an electronic communication held in electronic storage longer than 180 days requires either a valid search warrant,⁶¹ a subpoena,⁶² or a court order under Section 2703(d).⁶³

A 2703(d) order is based on "specific and articulable facts" that show reasonable grounds to believe an electronic communication is relevant and material to an ongoing criminal investigation.⁶⁴ The Supreme Court has said that specific and articulable facts, or reasonable suspicion, is more than a "hunch,"⁶⁵ but is nonetheless quantitatively and qualitatively "a less

⁴⁷ Carroll v. United States, 267 U.S. 132 (1925).

⁴⁸ Katz v. United States, 389 U.S. 347, 351 (1967).

⁴⁹ Smith v. Maryland, 442 U.S. 735 (1979).

⁵⁰ Schmerber v. California, 384 U.S. 757, 769-70 (1966).

⁵¹ Silverman v. United States, 365 U.S. 505, 511 (1961).

⁵² Hoffa v. United States, 385 U.S. 293, 301 (1966).

⁵³ 18 U.S.C. § 1702.

⁵⁴ Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

⁵⁵ United States v. Miller, 425 U.S. 435, 442-444 (1976).

⁵⁶ Smith v. Maryland, 442 U.S. 735, 742 (1979).

⁵⁷ Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

⁵⁸ H.R. Res. 4952, 99th Cong. (1986) (enacted).

⁵⁹ 18 U.S.C. § 2703.

⁶⁰ 18 U.S.C. § 2703(a).

⁶¹ 18 U.S.C. § 2703(b)(1)(A).

⁶² 18 U.S.C. § 2703(b)(1)(B)(i).

⁶³ 18 U.S.C. § 2703(d).

⁶⁴ 18 U.S.C. § 2703(d).

⁶⁵ Terry v. Ohio, 392 U.S. 1, 27 (1968).

demanding standard than probable cause."⁶⁶ Thus, in today's world, Section 2703(d) authorizes the federal government to compel an ECS or RCS provider, like Google, to disclose the content of electronic communications, such as opened e-mails or unopened e-mails held in storage longer than 180 days, without obtaining a warrant or showing probable cause..⁶⁷

Provider Type	Storage Time	Legal Process	Factual Standard
Electronic Communications Service ("ECS") provider	Less than or equal to 180 days	Valid search warrant	Probable cause
Electronic Communications Service ("ECS") provider	More than 180 days	Notice and subpoena; or Notice and 2703(d) order	Reasonable suspicion
Remote Computing Service ("RCS") provider	Not applicable	Notice and subpoena; or Notice and 2703(d) order	Reasonable suspicion

Prior to September 1, 2013, the laws of the state of Texas for government access to electronic communications essentially mirrored the ECPA. Article 18.21 of the Code of Criminal Procedure established in state law the same standards government must meet under federal law for the compelled disclosure of electronic communications by ECS providers and RCS providers. Similar to Section 2703(d), Sec. 5(a) of Article 18.21 requires that a court issue an order for the disclosure of the content of an electronic communication held in electronic storage when there is a "reasonable belief that the information sought is relevant to a legitimate law enforcement inquiry."⁶⁸ Like federal law, Texas law formerly authorized the forced disclosure of the content of electronic communications by an ECS and RCS provider to the government without a warrant or a showing of probable cause. This meant that "Texas law enforcement officials could seize opened email no matter its age, unopened email more than 180 days old, and documents, calendars, pictures, and other information that Texans stored in the cloud."⁶⁹

Technological advances in electronic communications and storage, such as e-mail, have frustrated the intent Congress expressed by passing the ECPA. In 1986, when an e-mail was opened, it was purged from the server and its content downloaded to the computer used to open

⁶⁶ Alabama v. White, 496 U.S. 325, 330 (1990).

⁶⁷ 18 U.S.C. § 2703(b), (d).

⁶⁸ Tex. Code of Criminal Procedure Art. 18.21 § 5.

⁶⁹ *One Giant Leap for Privacy: Texas Now Requires a Warrant for Content*, Center for Democracy & Technology (June 18, 2013), <https://cdt.org/blog/one-giant-leap-for-privacy-texas-now-requires-a-warrant-for-content/>

it. That computer was likely kept at home because it was significantly bigger in size, heavier in weight, and much less mobile than the average computer today. When writing the ECPA, Congress knew the Fourth Amendment protected homes from unreasonable government searches and, consequently, reasonably thought that, when the ECPA passed, most opened e-mails were constitutionally protected because they were most likely located on a computer in a home. Today, however, e-mails, documents, calendars, pictures, and vast amounts of other information are stored on distant third-party servers known as "the cloud" where the Fourth Amendment doesn't protect them because of the Third Party Doctrine. Despite congressional intent to the contrary, the letter of the law presently makes electronic communications legally susceptible to government intrusion without a valid search warrant or a demonstration of probable cause.

Not satisfied with federal law on this issue, lawmakers in Washington, D.C. have introduced bipartisan legislation to reform the ECPA. According to United States Senator Patrick Leahy, "the ECPA has become outdated by vast technological advances and changing law enforcement missions," which is why he introduced the Electronic Communications Privacy Act Amendments Act of 2013 (S. 607) with Senator Mike Lee, Senator Rand Paul, and Senator Jerry Moran.⁷⁰ The bill would "update the privacy protections for e-mail and other electronic communications" to require a valid search warrant for their disclosure by an ECS or RCS provider to the government, regardless of the age of the communication or whether it has been opened.⁷¹ The legislation would also require the government to provide notice and a copy of the search warrant to the individual whose communication was disclosed within ten business days of the government's receipt of the communication.⁷² Although S. 607 has been reported out of the Senate Committee on the Judiciary and is awaiting action on the floor of the United State Senate, the legislation has little chance of passing before the end of the 113th Congress.⁷³

Legislative reform efforts in Texas have been more successful than those in Washington, D.C. On June 14, 2013, Texas Governor Rick Perry signed House Bill 2268,⁷⁴ which amended Article 18.21 of the Code of Criminal Procedure to require a valid search warrant for the disclosure of the content of electronic communications held in electronic storage by ECS and RCS providers to an authorized peace officer of the State of Texas and its political subdivisions, such as county constables and municipal law enforcement.⁷⁵ The bill also prohibits state and local law enforcement from receiving a 2703(d) order for the disclosure of the content of electronic communications because, under the SCA, a 2703(d) order does not issue to a "state governmental entity" if prohibited by the laws of that state.⁷⁶ Unlike the ECPA, Texas law no longer authorizes the forced disclosure of the content of electronic communications held in

⁷⁰ *Summary of the Electronic Communications Privacy Act Amendments Act of 2013*, Official U.S. Senate website of Senator Patrick Leahy, <http://www.leahy.senate.gov/download/section-by-section-ecpa-reform-bill> (last visited Dec. 11, 2014).

⁷¹ *Id.*

⁷² *Id.*

⁷³ *S.607 - Electronic Communications Privacy Act Amendments Act of 2013*, Congress.gov, <https://www.congress.gov/bill/113th-congress/senate-bill/607> (last visited Dec. 11, 2014).

⁷⁴ *Tex. House Journal*, 83rd Leg., Regular Sess., 14 June 2013 (pg. 5442).

⁷⁵ *Tex. Code of Criminal Procedure Art. 18.21 § 4(a)*.

⁷⁶ *18 U.S.C. § 2703(d)*.

electronic storage without a valid search warrant supported by a showing of probable cause.⁷⁷ According to the Center for Democracy and Technology this is particularly important because "Texas beat U.S. Congress to the punch by updating its own electronic privacy laws first by requiring a warrant for law enforcement access to stored communications content."⁷⁸ Nevertheless, there remains one major way in which Texas law and the ECPA are alike. Like federal law, Texas law still sanctions the compelled disclosure of non-content and basic subscriber information, such as the subscriber's name, address, and telephone connection records without a valid search warrant or a showing of probable cause.^{79 80}

Under the ECPA and Article 18.21 prior to its amendment, the federal government and Texas peace officers were allowed access to the content of electronic communications held in electronic storage without a valid search warrant. This statutory authority, however, wasn't the only manner in which government legally accessed private digital content. On August 22, 2009, David Riley was pulled over by police in San Diego, California for operating a vehicle with an expired license registration.⁸¹ Soon thereafter it was discovered that Mr. Riley was also driving with an expired driver license.⁸² Pursuant to the policy of the San Diego Police Department, Mr. Riley was arrested and his car impounded.⁸³ Mr. Riley had his cell phone in his pocket when he was arrested, which the police seized and searched.⁸⁴ The search produced evidence implicating Mr. Riley in a suspected gang shooting earlier that month.⁸⁵ At the time, the search of Mr. Riley's cell phone was warrantless and not authorized by any statute, but was thought to be lawful pursuant to the common law exception for a search incident to a lawful arrest.⁸⁶ Because Mr. Riley's arrest was lawful, the San Diego police thought the search would be as well. However, the Supreme Court disagreed.⁸⁷ In *Riley v. California*, the Court held that the cell phone could not be searched incident to arrest because its digital data cannot be used as a weapon to physically harm a police officer or to help a suspect escape.⁸⁸ Ultimately, the Court ruled that the Fourth Amendment should protect cell phones and similar mobile devices because:

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.⁸⁹

⁷⁷ Tex. Code of Criminal Procedure Art. 18.21 § 5A(a).

⁷⁸ *One Giant Leap for Privacy: Texas Now Requires a Warrant for Content*, Center for Democracy & Technology (June 18, 2013), <https://cdt.org/blog/one-giant-leap-for-privacy-texas-now-requires-a-warrant-for-content/>

⁷⁹ Tex. Code of Criminal Procedure Art. 18.21 § 4(b).

⁸⁰ 18 U.S.C. § 2703(c).

⁸¹ *Riley v. California*, 134 S. Ct. 2473, 2477 (2014).

⁸² *Id.*

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ *Id.*

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ *Id.* at 2495-96.

The Court's decision in *Riley* and House Bill 2268 prohibit Texas government from forcing the disclosure of digital data or the content of electronic communications without a warrant. Nevertheless, Texas government may continue to be able to legally obtain access to so-called geolocation data without a warrant or a showing of probable cause under Sec. 5 of Article 18.21, which requires that a court order the disclosure of a "wire or electronic communication...if the court determines there is reasonable belief the information sought is relevant to a legitimate law enforcement inquiry."⁹⁰ Geolocation is "the process...of identifying the geographical location of a person or device by means of digital information processed via the Internet."⁹¹ One type of geolocation data is "historic cell-site location" data, which is the information a cellular provider for a particular mobile device, such as a cellular phone, receives when that device sends a signal to a cellular tower operated by the cellular provider. Historic cell-site location data can be used to estimate the location of a device "based on the network antenna to which the phone is connected."⁹² According to the Center for Democracy and Technology, "each time a cell phone communicates with an antenna, the wireless carrier records the cell-site identifier" and since "carriers know the precise latitude and longitude of all or almost all of their antennas, the cell-site identifier can be translated into the GPS coordinates..."⁹³ Texas law enforcement often obtains this record without a valid search warrant or a showing of probable cause and uses it to track the past movements of an individual suspected of committing a crime..⁹⁴

A bill from the 83rd Legislative Session would have ended this warrantless practice..⁹⁵ House Bill 1608, authored by Representative Hughes and coauthored by more than 100 members of the Texas House of Representatives, would have required a valid search warrant supported by probable cause for the disclosure of historic cell-site location data by a cellular provider to Texas law enforcement, such as the Department of Public Safety, a county constable, or a municipal police department..⁹⁶ House Bill 1608 was considered in a formal hearing of the House Committee on Criminal Jurisprudence on March 26, 2013..⁹⁷ During that hearing five (5) arguments were presented against House Bill 1608 by the law enforcement community and countered by privacy advocates. An additional argument has arisen since the end of the 83rd Regular Session, which focuses on the law following passage of House Bill 2268.

The first argument made by law enforcement representatives stated that requiring a valid search warrant for the disclosure of historic cell-site location data would remove an important "tool" from the law enforcement "toolbox" and thereby decrease their ability to solve crime, apprehend

⁹⁰ Tex. Code of Criminal Procedure Art. 18.21 § 5(a).

⁹¹ *Geolocation Definition*, OxfordDictionaries.com,

http://www.oxforddictionaries.com/us/definition/american_english/geolocation (last visited Dec. 11, 2014).

⁹² Center for Democracy and Technology, *Cell Phone Tracking: Trends in Cell Site Precision* (April 22, 2013),

<https://www.cdt.org/files/file/cell-location-precision.pdf>

⁹³ *Id.*

⁹⁴ Senate Committee on State Affairs hearing, Sept. 16, 2014 (Testimony of James Taylor, Houston Police Department).

⁹⁵ H.B. 1608, 83rd Leg., Regular Sess. (Tex. 2013).

⁹⁶ *Id.*

⁹⁷ *H.B. 1608 History*, Texas Legislature Online,

<http://www.capitol.state.tx.us/BillLookup/History.aspx?LegSess=83R&Bill=HB1608> (last visited Dec. 11, 2014).

criminal suspects, and prosecute those charged with committing a crime.⁹⁸ This point was echoed at a Senate Committee on State Affairs hearing on September 16, 2014. At that hearing, law enforcement claimed they "cannot respond timely to significant investigations" when a valid search warrant is required to obtain historic cell-site location data.⁹⁹ Privacy advocates, such as the American Civil Liberties Union (ACLU) and the Electronic Privacy Coalition, responded by noting the purpose of the Fourth Amendment is not intended to ensure the effectiveness of law enforcement efforts to combat criminal activity, but rather to guarantee that those efforts do not violate the rights of the citizenry.¹⁰⁰ Furthermore, privacy advocates pointed out that House Bill 1608 would not have prevented law enforcement from timely responding to significant investigations because the bill exempted kidnappings, hostage situations, and other "immediate life-threatening situations" from the warrant requirement.¹⁰¹

Secondly, law enforcement argued the Fourth Amendment does not protect historic cell-site location data so neither should state law, maintaining that a person has no reasonable expectation of privacy in historic cell-site location data because it is a business record of a transaction voluntarily revealed to a third-party cellular provider.¹⁰² The Texas Fourth Court of Appeals reached a similar conclusion in *Ford v. State*.¹⁰³ In that case, the court was confronted with the issue of whether the Fourth Amendment was violated by the warrantless acquisition of historic cell-site location data by the State of Texas.¹⁰⁴ In ruling that the Fourth Amendment was not violated, the court said historic cell-site location data are "simply business records" in which there is no "reasonable expectation of privacy" because they are "voluntarily conveyed to a third party."¹⁰⁵ Alternatively, privacy advocates contended that while historic cell-site location data is not currently protected by the Fourth Amendment, it should be safeguarded under state law because location information is personal, unique, and bares a "comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."¹⁰⁶

Next, law enforcement representatives argued that since historic cell-site location information only reveals the past location of a particular mobile device, and not necessarily the previous whereabouts of a specific individual, state law should not require a warrant for its disclosure.¹⁰⁷ Privacy advocates, conversely, emphasized the reality that mobile devices are increasingly

⁹⁸ House Committee on Criminal Jurisprudence hearing, March 26, 2013 (See generally testimony of law enforcement representatives).

⁹⁹ *Id.*

¹⁰⁰ House Committee on Criminal Jurisprudence hearing, March 26, 2013 (Testimony of Dr. Christopher Soghoian, American Civil Liberties Union).

¹⁰¹ House Committee on Criminal Jurisprudence hearing, March 26, 2013 (Testimony of Scott Henson, Electronic Privacy Coalition).

¹⁰² House Committee on Criminal Jurisprudence hearing, March 26, 2013 (See generally testimony of law enforcement representatives).

¹⁰³ *Ford v. State*, No. 04-12-00317-CR, 2014 Tex. Ct. App. (2014).

¹⁰⁴ *Id.*

¹⁰⁵ *Id.*

¹⁰⁶ *United States v. Jones*, 132 S. Ct. 945, 955 (2012).

¹⁰⁷ House Committee on Criminal Jurisprudence hearing, March 26, 2013 (See generally testimony of law enforcement representatives).

becoming a surrogate means of determining a person's location.¹⁰⁸ They point to a 2013 Harris Interactive Poll on mobile consumer habits that found "nearly three quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."¹⁰⁹

The fourth position law enforcement took at the hearing for House Bill 1608 was that historic cell-site location data does not provide pinpoint precision for the location of a person or their mobile device, and therefore should not require a warrant for its disclosure.¹¹⁰ In response, privacy advocates explained the exactness of historic cell-site location data depends on the range of the nearest cellular tower, which theoretically can serve an area up to ten square miles.¹¹¹ Yet, each individual cellular tower can only manage a certain amount of network traffic, such as calls or Internet usage, and in the average ten-square-mile urban area, the network traffic will exceed the capacity of a single cellular tower.¹¹² When this happens, a typical cellular provider will install another cellular tower, or as many cellular towers as necessary, to manage the excess network traffic.¹¹³ This necessarily reduces, according to privacy advocates, the service area for each cellular tower.¹¹⁴ They contend that the result of installing each new cellular tower is that historic cell-site location data becomes increasingly more precise.¹¹⁵ In the last 15 years, the number of cells-sites has grown more than 450 percent from 65,887 cellular towers in December 1998 to nearly 305,000 in December of last year.¹¹⁶ ¹¹⁷ Due to this increase, "some of these cell-sites cover very small areas, and the location information indicated by these sites can be as precise as that generated by GPS."¹¹⁸ According to the Electronic Privacy Information Center historic cell-site location data has become so precise it can be used to locate a device in a neighborhood or on a particular block, or it can be used to pinpoint a device in a specific building or room.¹¹⁹

¹⁰⁸ House Committee on Criminal Jurisprudence hearing, March 26, 2013 (Testimony of Dr. Christopher Soghoian, American Civil Liberties Union).

¹⁰⁹ *Riley v. California*, 134 S. Ct. 2473, 2490 (2014).

¹¹⁰ House Committee on Criminal Jurisprudence hearing, March 26, 2013 (See generally testimony of law enforcement representatives).

¹¹¹ Center for Democracy and Technology, *Cell Phone Tracking: Trends in Cell Site Precision* (April 22, 2013), <https://www.cdt.org/files/file/cell-location-precision.pdf>

¹¹² *Id.*

¹¹³ *Id.*

¹¹⁴ *Id.*

¹¹⁵ *Id.*

¹¹⁶ CTIA-The Wireless Association, *2014 Annual Wireless Industry Survey*, <http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey> (last visit Dec. 11, 2012).

¹¹⁷ This is a result of a significant increase in the number of wireless subscribers in the United States during the last 20 years. In 1995 there were only 33.8 million cellular subscribers in the United States. Today, there are more than 320 million cellular subscribers representing nearly ninety percent of U.S. households. Many of these subscribers are using smartphones, which create forty-nine percent more network traffic than a basic handset. From 2012 to 2013, the amount of data consumed by mobile devices doubled and is projected to increase 650 percent by 2018. This growth has prompted cellular providers in the U.S. to rapidly expand their networks. Last year, U.S. cellular providers invested \$33 billion in capital expenditures and have invested more than \$260 billion over the last decade.

¹¹⁸ Center for Democracy and Technology, *Cell Phone Tracking: Trends in Cell Site Precision* (April 22, 2013), <https://www.cdt.org/files/file/cell-location-precision.pdf>

¹¹⁹ Electronic Privacy Information Center, *Locational Privacy*, https://epic.org/privacy/location_privacy/ (last visited Dec. 11, 2014).



Retention Periods of Major Cellular Service Providers

Data gathered by the Computer Crime and Intellectual Property Section, U.S. Department of Justice

	Verizon	T-Mobile	AT&T/Cingular	Sprint	Nextel	Virgin Mobile ¹
Subscriber Information:	Post-paid: 3-5 years*	5 years	Depends on length of service	Unlimited	Unlimited	Unlimited
Call detail records:	1 rolling year	Pre-paid: 2 years Post-paid: 5 years	Pre-paid: varies Post-paid: 5-7 years	18-24 months	18-24 months	2 years
Cell towers used by phone:	1 rolling year	Officially 4-6 months, really a year or more.	From July 2008	18-24 months	18-24 months	Not retained - obtain through Sprint
Text message detail:	1 rolling year	Pre-paid: 2 years Post-paid: 5 years	Post paid: 5-7 years	18 months (depends on device)	18 months (depends on device)	60-90 days
Text message content:	3-5 days	Not retained	Not retained	Not retained	Not retained	90 days (search warrant required with "text of text" request)
Pictures:	Only if uploaded to website (customer can add or delete pictures any time)	Can be stored online and are retained until deleted or service is canceled	Not retained	Contact provider	Contact provider	Not retained
IP session information:	1 rolling year	Not retained	Only retained on non-public IPs for 72 hours. If public IP, not retained.	60 days	60 days	Not retained
IP destination information:	90 days	Not retained	Only retained on non-public IPs for 72 hours. If public IP, not retained.	60 days	60 days	Not retained
Bill copies (post-paid only):	3-5 years, but only last 12 months readily available	Not retained	5-7 years	7 years	7 years	n/a [‡]
Payment history (post-paid only):	3-5 years, check copies for 6 months*	5 years	Depends on length of service	Unlimited	Unlimited	n/a [‡]
Store Surveillance Videos:	Typically 30 days	2 weeks	Depends. Most stores carry for 1-2 months	Depends	Depends	n/a
Service Applications:	Post-paid: 3-5 years*	Not retained	Not retained	Depends	Depends	Not retained

* May vary by former company

** For records older than mid-Nov. 2007, Sprint can only provide bill reprints with outgoing info

‡ No bill copies, but list of credit card transactions does not expire.

¹ Virgin Mobile is now owned by Sprint. Since companies have separate compliance offices, for now they are listed separately.

August 2010

Law Enforcement Use Only

Source: American Civil Liberties Union

Law enforcement also argued that requiring a valid search warrant would waste valuable police resources and result in the destruction of evidence, because the time required to obtain a search warrant for the disclosure of historic cell-site location data is often longer than the length of time the records for that data are retained by cellular providers.¹²⁰ This point is forcefully disputed by privacy advocates.¹²¹ They argue, based on a document acquired from the Department of Justice ("DOJ") under the Freedom of Information Act, that many cellular providers retain historic cell-site location data for years.¹²² According to that document, Sprint retains historic cell-site location data for 18-24 months and AT&T hasn't destroyed any historic cell-site location data since July 2008 (see below).

Lastly, law enforcement representatives (primarily district attorney's offices), have begun to argue that House Bill 2268 unexpectedly changed state law to require a valid search warrant supported by probable cause to force a cellular provider to disclose records of historic cell-site location data under Article 18.21 of the Code of Criminal Procedure. Privacy advocates assert that House Bill 2268 only applies to "electronic customer data," which is defined as including the "the content of a wire communication or electronic communication sent to or by the customer." Since historic cell-site location data is not content, House Bill 2268 did not change the legal standard required for its disclosure, which privacy advocates insist continues to be a subpoena or a court order based on a "reasonable belief that the [historic cell-site location] information sought is relevant to a legitimate law enforcement inquiry" under Sec. 5 of Article 18.21. The law is clearer in other states, such as Utah, where Governor Gary Herbert signed House Bill 128 on March 31 requiring "that a governmental entity obtain a search warrant before obtaining the location information of an electronic device."¹²³ The bill also bans "the admission of electronic data collected without a warrant in criminal court proceedings."¹²⁴ Legislatures in Virginia,¹²⁵ Montana,¹²⁶ Tennessee,¹²⁷ Missouri,¹²⁸ and New Hampshire¹²⁹ have all proposed or passed similar measures requiring a search warrant for a government entity to obtain location information of an electronic device.

A law enforcement technique to gather evidence and make arrests that has not been debated by the Legislature is the use StingRays. Also known as a cell-site simulator or IMSI-catcher, a StingRay is a device that transmits signals that mimic a cellular tower of a wireless carrier, such as AT&T, Sprint, or Verizon, to trick nearby cellular devices, such as an iPhone or an iPad, into

¹²⁰ House Committee on Criminal Jurisprudence hearing, March 26, 2013 (See generally testimony of law enforcement representatives).

¹²¹ Senate Committee on State Affairs hearing, Sept. 16, 2014 (Testimony of Dr. Christopher Soghoian, American Civil Liberties Union).

¹²² *Id.*

¹²³ H.B. 128, 2014 Gen. Sess. (Utah 2014).

¹²⁴ *Id.*

¹²⁵ H.B. 17, 2014 Gen. Sess. (Va. 2014) (enacted).

¹²⁶ H.B. 603, 63rd Sess. (Mt. 2013) (enacted).

¹²⁷ S.B. 2087, 108th Gen. Ass. (Ten. 2014).

¹²⁸ H.B. 1388, 97th Gen. Ass., 2nd Reg. Sess. (Mo. 2014).

¹²⁹ H.B. 1567, 2014 Reg. Sess. (NH. 2014).

transmitting back to the StingRay.¹³⁰ This reciprocated transmission can be manipulated to capture the identifying information of a cellular device, such as an IMSI number or Electronic Serial Number (ESN), and to track the location of the transmitting cellular device to within ten feet of its actual location, even when the cellular device is not being used.¹³¹ Additionally, a StingRay can intercept the content of communications from certain cellular devices by launching a "man-in-the-middle attack," where the StingRay pretends to be a cell-site tower and then pretends to be a particular mobile device so that signals between the cellular device and a legitimate cell-site tower flow to, and through, the StingRay.¹³²

StingRay technology was initially developed for the United States military, but is now also used by several federal, state, and local law enforcement agencies.¹³³ As many as eight state law enforcement agencies and sixteen local police departments own a StingRay or a more advanced version.¹³⁴ In Texas, a StingRay has been purchased and used by the Fort Worth Police Department (FWPD),¹³⁵ the Houston Police Department (HPD),¹³⁶ and the Texas Department of Public Safety (DPS).¹³⁷ The federal government has funded most StingRay purchases by these state and local law enforcement agencies with anti-terrorism grants through the Department of Homeland Security.¹³⁸ As a condition for receiving those grants, state and local police often sign a non-disclosure agreement, including the FWPD, HPD, and DPS. Thus very little is known about how StingRays have been used in Texas.

Law enforcement representatives claim that StingRays are only used to collect evidence or make arrests for serious crimes and in emergency situations, such as to track the location of the cellular device of a person suspected of murder, kidnapping, or drug smuggling. Privacy advocates, however, are highly skeptical of that claim. According to the Electronic Frontier Foundation, the Los Angeles Police Department has been using its StingRay "for just about any investigation imaginable."¹³⁹ The ACLU is also concerned about the use of StingRays by law enforcement for several reasons. First, they are concerned because a StingRay often captures private information

¹³⁰ Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, Wall Street Journal, Nov. 13, 2014, http://www.wsj.com/news/article_email/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533-IMyQjAxMTI0NTEwNDxMTQwWj

¹³¹ *Id.*

¹³² *Id.*

¹³³ American Civil Liberties Union, *Stingray Tracking Devices: Who's Got Them?*, <https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them> (last visited Dec. 11, 2014).

¹³⁴ *Id.*

¹³⁵ Andrew Tanielian, *Fort Worth Cellphone Tracker Rings Controversy*, Channel 5 NBCDFW.com, Feb. 9, 2012, <http://www.nbcdfw.com/news/local/Fort-Worth-Cellphone-Tracking-Rings-Controversy-140796693.html>

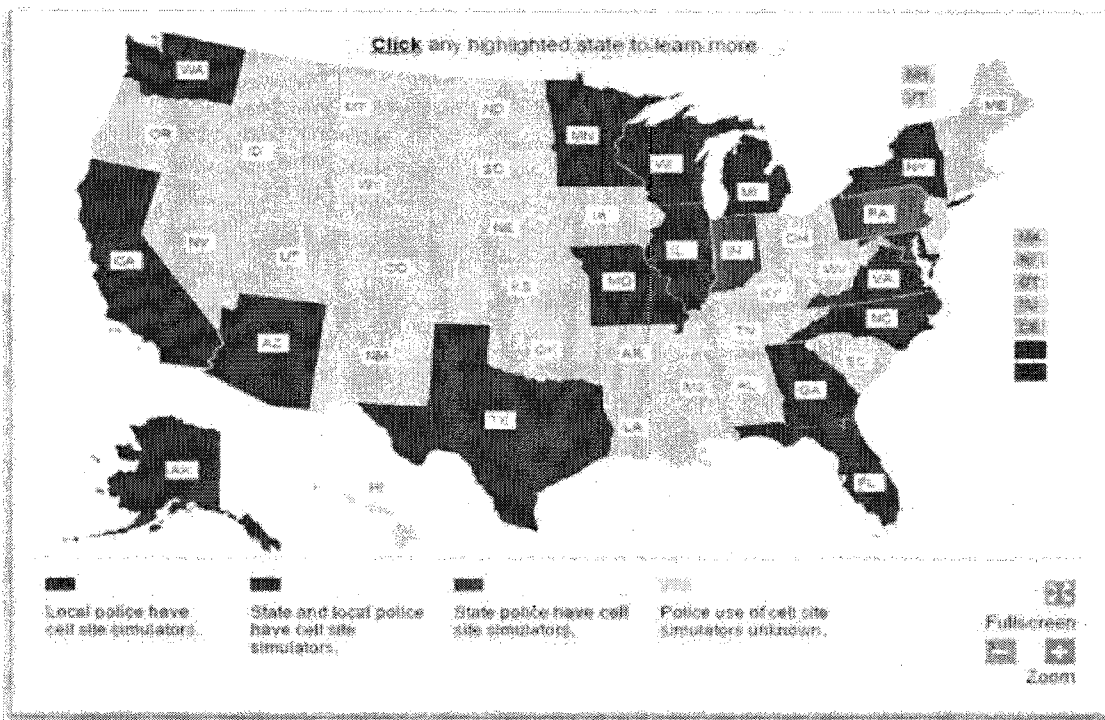
¹³⁶ Houston City Council Agenda, NO. 2012-0733-1, Pg. 13 (Oct. 16, 2012) <http://www.houstontx.gov/citysec/agendas/2012/20121016.pdf>

¹³⁷ John Anderson, *APD: Can We Please Buy Some Top-Secret "StingRays"?*, The Austin Chronicle, Oct. 17, 2014, <http://www.austinchronicle.com/news/2014-10-17/apd-can-we-please-buy-some-top-secret-stingrays/>

¹³⁸ Steven Lawson, *California police criticized for 'stingray' cellphone trackers*, PCWorld, March 13, 2014, <http://www.pcworld.com/article/2108320/california-police-criticized-for-stingray-cellphone-trackers.html>

¹³⁹ Harriet Arkell, *'An unconstitutional, all-you-can-eat data buffet': Critics slam FBI's Stingray mobile tracking tool*, Mail Online, Feb. 13, 2013, <http://www.dailymail.co.uk/sciencetech/article-2278110/Critics-slam-FBI-s-unconstitutional-Stingray-mobile-tracking-tool.html>

from third parties, not just the target of a police investigation.¹⁴⁰ Their second concern is that a StingRay broadcasts electronic signals up to several kilometers that penetrate the walls of private spaces, such as a homes or office, allowing the StingRay to capture intimate data from private locations within a fairly large area.¹⁴¹ Another concern is that a StingRay forces cell phones to transmit signaling information.¹⁴² As one law enforcement officer described it, a StingRay “actually captures the phone” and “direct[s] the signal from the [carrier’s] tower to [the government’s] equipment.”¹⁴³ Lastly, it concerns the ACLU that neither a warrant or a showing of probable cause is required by Texas or federal law to use a StingRay or similar device.¹⁴⁴



Source: American Civil Liberties Union

Any necessary protections against non-consented video and audio recordings collected by private handheld and wearable mobile devices and other private surveillance.

Furthermore, no one can feel sure at any moment that a camera has not been brought to bear upon him. If a young man and a young woman sit down side-by-side in an apparently quiet nook among the sand dunes, or by a mountain stream, it will not be ten minutes before a dozen or fifteen cameras will be trained upon them. Even when walking quietly in the public street a person is not safe, for not only is he constantly made the victim of the instantaneous process by

¹⁴⁰ Linday Lye, *Stringrays: The Most Common Surveillance Tool the Government Won't Tell you About*, American Civil Liberties Union of Northern California, June 27, 2014, available at https://www.aclunc.org/sites/default/files/StingRays_The_Most_Common_Surveillance_Tool_the_Govt_Won%27t_Tell_You_About.pdf

¹⁴¹ *Id.*

¹⁴² *Id.*

¹⁴³ *Id.*

¹⁴⁴ *Id.*

camera lunatics concealed behind window curtains, but the inoffensive theological student with what is apparently an innocent handbag in his hand, who passes slowly along the street, may have a camera disguised as a handbag and may be taking 'instantaneous views' without exciting the slightest suspicion. Things have come to such a pass that no lady can step out of a carriage without the fear that every stripe has been surreptitiously caught by a shameless camera...

- Excerpt from *The Camera Epidemic*, published in *New York Times* on August 20, 1884

In the late 1880s, modern photography was born when George Eastman invented photographic film and the Kodak camera.¹⁴⁵ By 1900, Eastman was selling a reasonably-sized camera for only \$1, which is roughly \$29 when inflation adjusted.¹⁴⁶ Small and affordable, Eastman had trouble keeping up with demand. As more people purchased cameras and began taking pictures, privacy concerns arose. An article published by the *New York Times* in August 1884 referred to the use of a camera as an "epidemic" and equated it to cholera.¹⁴⁷ Today, cameras and camcorders are much smaller, more affordable, more widespread, and more concealable than in 1884. For example, a small phone with a 1.3 megapixel camera with digital zoom and video capability costs less than \$15.¹⁴⁸ Although not yet commercially available, Google Glass allows a person to wear a device capable of capturing crystal clear images and video on the bridge of their nose and atop their ears, like eyeglasses, and take pictures or videos by a voice command, light touch of the rims, or a blink of the eye.¹⁴⁹ Furthermore, an unmanned aerial vehicle (commonly known as a drone) allows a person to purchase for as little as several hundred dollars a camcorder affixed to a flying apparatus that can be remotely operated to capture images or video of people, places, or events, such as a family vacation.¹⁵⁰ These technological developments – camera phones, Google Glass, and drones – have made it much easier than ever to capture non-consented video and audio recordings, sometimes surreptitiously, and thus have reignited the pervasive privacy concerns caused by the invention and increasingly widespread use of cameras in the later part of the 19th Century.

The law defines consent generally as "a voluntary agreement to another's proposition or to voluntarily agree to an act or proposal of another."¹⁵¹ A person who consents has given "permission for something to happen" or is in "agreement to do something."¹⁵² Conversely, non-consent is an involuntary agreement, the absence of agreement, or the failure to gain permission. Thus, non-consented audio or audiovisual recordings are taken involuntarily without agreement,

¹⁴⁵ David Lindsay, *People & Events: George Eastman*, PBS.com, <http://www.pbs.org/wgbh/amex/eastman/peopleevents/pande02.html>

¹⁴⁶ *History of Kodak 1878-1929*, Kodak.com, http://www.kodak.com/ek/US/en/Our_Company/History_of_Kodak/Milestones_-_chronology/1878-1929.htm (last visited Dec. 11, 2014).

¹⁴⁷ *The Camera Epidemic*, *New York Times*, Aug. 20, 1884.

¹⁴⁸ Fifteen dollars is less than three hundredths of one percent of the median U.S. household income of \$51,017 in 2013.

¹⁴⁹ Hayley Tsukayama, *Everything you need to know about Google Glass*, *The Washington Post*, Feb. 27, 2014, <http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/27/everything-you-need-to-know-about-google-glass/>

¹⁵⁰ Geoffrey A. Fowler, *Let's Go Fly a Drone: The Best Vacation Pics Come From Above*, *The Wall Street Journal*, May 16, 2014, <http://www.wsj.com/articles/SB10001424052702304081804579560191717456938>

¹⁵¹ *Consent Definition*, Law.com, <http://dictionary.law.com/Default.aspx?selected=299> (last visited Dec. 11, 2014).

¹⁵² *Id.*

or without permission, for their capture. The law usually permits the recording of a conversation when all parties consent.¹⁵³ and presumes consent where the recording device is in the plain view, such as during face-to-face interviews.¹⁵⁴ The use of a hidden device, however, implicates state wiretapping laws when used to record audio or audiovisual. The law in forty-nine states requires at least one party's consent to a surreptitious audio or audiovisual recording of a conversation.¹⁵⁵ In thirty-eight of those states, an audio or audiovisual recording is legal with the consent of only one party.¹⁵⁶ These states are known as "one-party" states.¹⁵⁷ The other eleven states, including California and Illinois, require that all parties consent to the audio or audiovisual recording for it to be captured lawfully.¹⁵⁸ These states are referred to as "two-party" states.¹⁵⁹

A considerable issue in two-party states involves filming the police. In Massachusetts, a two-party state, there are reports that several people have been arrested for taking an audiovisual recording of on-duty law enforcement officers and charged with "illegal electronic surveillance" because the officers didn't consent to the capturing of the video.¹⁶⁰ Consider this excerpt from an article published by the Boston Globe on January 12, 2010 titled "Police fight cellphone recordings":

Simon Glik, a lawyer, was walking down Tremont Street in Boston when he saw three police officers struggling to extract a plastic bag from a teenager's mouth. Thinking their force seemed excessive for a drug arrest, Glik pulled out his cell phone and began recording. Within minutes Glik said he was in handcuffs. 'One of the officers asked me whether my phone had audio recording capabilities,' Glik, 33, said recently of the incident, which took place in October 2007. Glik acknowledged that it did and then, he said, 'my phone was seized, and I was arrested.' The charge? Illegal electronic surveillance.¹⁶¹

During the 83rd Regular Session of the Texas Legislature, Senate Bill 897 was introduced to confirm that it is lawful for Texas citizens to film, record, photograph, document, and observe on-duty peace officers in the state.¹⁶² The bill was considered by the Senate Committee on State

¹⁵³ Digital Media Law Project, *Recording Phone Calls and Conversations*, <http://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations> (last visited Dec. 11, 2014).

¹⁵⁴ Reporters Committee for Freedom of the Press, *Reporter's Recording Guide*, <http://www.rcfp.org/rcfp/orders/docs/RECORDING.pdf> (last visited Dec. 11, 2014).

¹⁵⁵ Digital Media Law Project, *Recording Phone Calls and Conversations*, <http://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations> (last visited Dec. 11, 2014).

¹⁵⁶ *Id.*

¹⁵⁷ Digital Media Law Project, *Texas Recording Law*, <http://www.dmlp.org/legal-guide/texas-recording-law> (last visited Dec. 11, 2014).

¹⁵⁸ Digital Media Law Project, *Recording Phone Calls and Conversations*, <http://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations> (last visited Dec. 11, 2014).

¹⁵⁹ *Id.*

¹⁶⁰ Daniel Rowinski, *Police fight cellphone recordings*, *The Boston Globe*, January 12, 2010, http://www.boston.com/news/local/massachusetts/articles/2010/01/12/police_fight_cellphone_recordings/

¹⁶¹ *Id.*

¹⁶² S.B. 897, 83rd Leg., Regular Sess. (Tex. 2013).

Affairs in a public hearing on April 29, 2013, but was left pending until session ended on May 27 of the same year.¹⁶³

Unlike Massachusetts, Texas is a one-party state.¹⁶⁴ Under the Texas wiretapping statute, it is a criminal offense to intercept or record any "wire, oral, or electronic communication"¹⁶⁵ unless at least one party consents to the taping or filming.¹⁶⁶ The person consenting can be the same person capturing the audio or audiovisual recording of the conversation, if that person is also a party to the conversation.¹⁶⁷ If not a party to the conversation, the person taping or filming must obtain the prior consent of at least one of the parties to the conversation.¹⁶⁸ The law does not, however, require consent to take an audio or audiovisual recording for every communication. Texas law does not protect the oral communications of parties who do not have an "expectation that such communication is not subject to interception under circumstances justifying such expectation."¹⁶⁹ Put differently, the Texas wiretapping law does not apply to conversations in which there is no reasonable expectation of privacy.¹⁷⁰ So, under Texas law, a person may be able to, without consent, take an audio or audiovisual recording of a conversation occurring in a public place, such as a public sidewalk, an aisle of a grocery store, or while waiting in line at the post office. A violation of Texas' wiretapping statute is punishable by 2-20 years imprisonment (i.e. state jail felony or felony of the second degree), a fine up to \$10,000, or both.¹⁷¹

In addition to the wiretapping statute, Texas law recognizes a cause of action for the violation of a person's right to privacy.¹⁷² Under the Second Restatement of Law of Torts, liability for that cause of action requires a highly offensive physical or nonphysical intrusion upon the solitude or seclusion of another individual, or his or her private affairs.¹⁷³ The intrusion must be highly offensive to a reasonable person and can be physical, such as breaking into a home, or nonphysical, such as using binoculars to look through a window, wiretapping telephone wires, searching through a safe, or examining a private bank account.¹⁷⁴ This privacy tort was first recognized by the Texas Supreme Court in *Billings v. Atkinson*.¹⁷⁵ In that case, a telephone company employee placed a wiretap on the residential telephone line of a customer and used the wiretap to listen to the personal conversations of the customer.¹⁷⁶ The court noted that, at the time, a majority of jurisdictions in the United States recognized a cause of action for the invasion

¹⁶³ *S.B. 897 History*, Texas Legislature Online,

<http://www.capitol.state.tx.us/BillLookup/History.aspx?LegSess=83R&Bill=SB897> (last visited Dec. 11, 2014)

¹⁶⁴ Digital Media Law Project, *Texas Recording Law*, <http://www.dmlp.org/legal-guide/texas-recording-law> (last visited Dec. 11, 2014).

¹⁶⁵ Tex. Penal Code § 16.02(b)(1).

¹⁶⁶ Tex. Penal Code § 1602(c)(4)(A)-(B).

¹⁶⁷ Digital Media Law Project, *Texas Recording Law*, <http://www.dmlp.org/legal-guide/texas-recording-law> (last visited Dec. 11, 2014).

¹⁶⁸ Texas Wiretapping Law in a Nutshell, Akin & Associates Forensics,

<http://www.akininc.com/PDFs/TEXAS%20WIRETAPPING%20LAW.pdf> (last visited Dec. 11, 2014).

¹⁶⁹ Tex. Code of Criminal Procedure Art. 18.20 § 1(2).

¹⁷⁰ *Id.*

¹⁷¹ Tex. Penal Code § 1602(f).

¹⁷² Restatement (second) of Torts § 652(B).

¹⁷³ *Id.*

¹⁷⁴ *Id.*

¹⁷⁵ *Billings v. Atkinson*, 489 S.W.2d 858 (1973).

¹⁷⁶ *Id.*

of privacy and held that "the right of privacy constitutes a legal injury for which a remedy will be granted."¹⁷⁷

The First Amendment to the United State Constitution and Article 1, Section 8 of the Texas Constitution prohibit Congress and the Texas Legislature from passing a law "abridging" or "curtailing" the freedom of speech.¹⁷⁸ ¹⁷⁹ On June 11, 2001, Governor Rick Perry signed House Bill 73 and a couple months later, on September 1, that bill became law.¹⁸⁰ House Bill 73 created the criminal offense of "improper photography or visual recording" in Section 21.15 of the Penal Code.¹⁸¹ From 2001 to 2003, a person committed this offense when a photograph or videotape of another person was taken "without the other person's consent and with the intent to arouse or gratify the sexual desire of any person."¹⁸² During the 78th Regular Session of the Texas Legislature in 2003, Section 21.15 of the Penal Code was amended by House Bill 1060.¹⁸³ That bill, signed by Governor Perry on June 20, 2003,¹⁸⁴ criminalized the "promotion" of an improper photograph or visual recording.¹⁸⁵ The statute was again amended in 2007 by House Bill 1804.¹⁸⁶ Signed by Governor Perry on June 15 of that year,¹⁸⁷ House Bill 1804 criminalized the broadcast or transmission of a visual image of another person without his or her consent and for the purpose of sexual gratification.¹⁸⁸ Section 21.15 was enforceable law until September 17, 2014.¹⁸⁹

On September 17, 2014, the Texas Court of Criminal Appeals struck down portions of Section 21.15 of the Penal Code as an unconstitutional violation of the right to free speech in *Ex parte Ronald Thompson*.¹⁹⁰ Several years ago, Ronald Thompson was charged with 26 counts of improper photography under Section 21.15 after taking underwater pictures of clothed children, most wearing swimsuits, at a San Antonio water park.¹⁹¹ Challenging the constitutionality of Section 21.15, Mr. Thompson argued the statute was overbroad and that a plain reading of the law would "place street photographers, entertainment journalists, arts patrons, pep rally attendees and 'even the harmless eccentric' at risk of incarceration."¹⁹² The court agreed and in an 8-1 ruling said:

¹⁷⁷ *Billings v. Atkinson*, 489 S.W.2d 858, 860 (1973).

¹⁷⁸ U.S. CONST. amend. I.

¹⁷⁹ T.X. Const. art. I, § 8.

¹⁸⁰ *Tex. House Journal*, 77th Leg., Regular Sess., 11 June 2001 (pg. 5217).

¹⁸¹ H.B. 73, 77th Leg., Regular Sess. (Tex. 2001) (enacted).

¹⁸² *Id.*

¹⁸³ H.B. 1060, 78th Leg., Regular Sess. (Tex. 2003) (enacted).

¹⁸⁴ *Tex. House Journal*, 78th Leg., Regular Sess., 20 June 2003 (pg. 6672).

¹⁸⁵ H.B. 1060, 78th Leg., Regular Sess. (Tex. 2003) (enacted).

¹⁸⁶ H.B. 1804, 80th Leg., Regular Sess. (Tex. 2007) (enacted).

¹⁸⁷ *Tex. House Journal*, 80th Leg., Regular Sess., 15 June 2007 (pg. 7405).

¹⁸⁸ H.B. 1804, 80th Leg., Regular Sess. (Tex. 2007) (enacted).

¹⁸⁹ *Ex parte Ronald Thompson*, NO. PD-1371-13, Tex. Ct. Crim. App. (2014).

¹⁹⁰ *Id.*

¹⁹¹ *Id.*

¹⁹² Cindy George, *Texas court throws out 'upskirt' photo law*, Houston Chronicle, Sept. 17, 2014,

<http://www.houstonchronicle.com/news/article/State-appeals-court-rules-upskirt-law-5763225.php?cmpid=twitter-premium&t=53c893b5408b7034ef>

*The camera is essentially the photographer's pen or paintbrush. Using a camera to create a photograph or video is like applying pen to paper to create a writing or applying brush to canvas to create a painting.... We conclude that a person's purposeful creation of photographs and visual recordings is entitled to the same First Amendment protection as the photographs and visual recordings themselves.*¹⁹³

The Court went on to also say that "protecting someone who appears in public from being the object of sexual thoughts seems to be the sort of 'paternalistic interest in regulating the defendant's mind' that the First Amendment was designed to guard against."¹⁹⁴ On the court's ruling, University of Houston constitutional law professor Peter Linzer said, "It's hard to see how you could make taking a picture a crime."¹⁹⁵ However, the Texas Legislature again restricted the lawful capture of images and video when Governor Rick Perry signed House Bill 912 into law on June 14, 2013.¹⁹⁶ Known as the "Texas Privacy Act," House Bill 912 established rules in Chapter 423 of the Government Code for the use of unmanned aircraft (i.e., drones) to capture images of private property and persons located on private property.¹⁹⁷ The Texas Privacy Act makes it a misdemeanor to use a drone "to capture an image of an individual or privately owned real property...with the intent to conduct surveillance" or to "possess, disclose, display, distribute, or otherwise use such an image."¹⁹⁸ Under the law, a person is subject to a fine not to exceed \$5,000 for the capture of all images associated with a single episode and a fine of up to \$10,000 for the disclosure of those images.¹⁹⁹ Actual damages can be awarded if the images are distributed with malice.²⁰⁰

As with drones, many are concerned about the potential privacy implications of Google Glass.²⁰¹ According to some, however, those concerns are unfounded for several reasons.²⁰² First, the reactions to Google Glass are similar to how people reacted to previous technological advancements that were not completely understood.²⁰³ For example, the first Kodak cameras "struck fear in the hearts of those who valued privacy" and were "banned from beaches after people sneaked photos of female sunbathers."²⁰⁴ Cameras were also, at one point, banned from the Washington Monument in Washington, D.C.²⁰⁵ As with cameras, some argue "we are being too quick to condemn groundbreaking technology [like Google Glass] that we don't understand

¹⁹³ *Ex parte Ronald Thompson*, NO. PD-1371-13, Tex. Ct. Crim. App. (2014).

¹⁹⁴ *Id.*

¹⁹⁵ Cindy George, *Texas court throws out 'upskirt' photo law*, Houston Chronicle, Sept. 17, 2014, <http://www.houstonchronicle.com/news/article/State-appeals-court-rules-upskirt-law-5763225.php?cmid=twitter-premium&t=53c893b5408b7034ef>

¹⁹⁶ Tex. *House Journal*, 83rd Leg., Regular Sess., 14 June 2013 (pg. 5441).

¹⁹⁷ H.B. 912, 83rd Leg., Regular Sess. (Tex. 2013) (enacted).

¹⁹⁸ *Id.*

¹⁹⁹ *Id.*

²⁰⁰ *Id.*

²⁰¹ Brad Keywell, *Fears of Google Glass Are Unfounded*, Time, May 22, 2013,

<http://ideas.time.com/2013/05/22/fears-of-google-glass-are-unfounded/>

²⁰² *Id.*

²⁰³ *Id.*

²⁰⁴ *Id.*

²⁰⁵ *Id.*

and haven't yet experienced."²⁰⁶ Second, state laws are in place to regulate covert recordings to protect privacy.²⁰⁷ The Texas wiretapping law and the intrusion upon seclusion tort recognized by Texas courts, both discussed above, are examples of such state laws. Lastly, Google Glass is not responsible for creating the capability to surreptitiously taping someone or something.²⁰⁸ For decades, a person has been able to purchase eyewear, a pen, or an MP3 player equipped with hidden cameras for a fraction of the price of Google Glass.²⁰⁹ Many are very concerned about the effect Google Glass may have on their privacy, yet those same people "would never think twice about someone wearing sunglasses or carrying a pen in their pocket."²¹⁰ Writing about Google Glass, Brad Keywell of Time Magazine, said, "When we don't understand something, we often react before grasping both the positive and negative implications."²¹¹

Necessary limits on warrantless monitoring of the physical location of individuals through the use of biometrics, RFID chips, facial recognition, or other technologies.

A biometric is a unique and measurable physical characteristic determined by the shape, color, and composition of the human body that is used to label, describe, and identify a person. Examples of a biometric include finger and palm prints, iris and retina scans, facial recognition, and deoxyribonucleic acid (DNA) samples.²¹² Biometrics are frequently used to secure government facilities, protect access to government computer networks, prevent fraud within government programs, screen people at borders, and fight crime.²¹³ They are often the most cost effective and reliable technique available to precisely and accurately verify a person's identity.²¹⁴ Other than DNA samples, which will be discussed under Interim Charge No. 3, Texas generally collects and stores only two types of biometrics used to identify people: fingerprints and photographs. A fingerprint sample is required to obtain a driver's license²¹⁵ and legally practice many occupations or professions.²¹⁶ A fingerprint sample is also routinely taken from a person arrested for a criminal offense as part of the booking process.²¹⁷ In addition to fingerprints, state government and local governments in Texas maintain or have access to a photographic database of driver license applicants and those booked for a suspected criminal offense (i.e., a mug shot).

²⁰⁶ Brad Keywell, *Fears of Google Glass Are Unfounded*, Time, May 22, 2013, <http://ideas.time.com/2013/05/22/fears-of-google-glass-are-unfounded/>

²⁰⁷ *Id.*

²⁰⁸ *Id.*

²⁰⁹ *Id.*

²¹⁰ *Id.*

²¹¹ *Id.*

²¹² National Science and Technology Council, *Introduction to Biometrics*, <http://www.biometrics.gov/ReferenceRoom/Introduction.aspx> (last visited Dec. 12, 2014).

²¹³ *Id.*

²¹⁴ *Id.*

²¹⁵ Dave Lieber, *Watchdog: Driver's license centers snatch your fingerprints*, June 19, 2014, <http://www.dallasnews.com/investigations/watchdog/20140607-watchdog-drivers-license-centers-snatch-your-fingerprints.ece>

²¹⁶ Mike Riggs, *Texas Architects Will Soon Have to Be Fingerprinted*, Dec. 10, 2013, <http://www.citylab.com/work/2013/12/texas-architects-will-soon-have-be-fingerprinted/7825/>

²¹⁷ Code of Criminal Procedure Art. 60.08(b).

The government collection of biometrics in Texas has raised privacy concerns regarding the ultimate use of the information.²¹⁸ However, there are rules under Texas law for the capture, use and disclosure of a "biometric identifier" by a "governmental body"²¹⁹ or a person for a "commercial purpose."²²⁰ According to University of Houston law professor Ronald Scott, "Texas law protects the confidentiality of an individual's biometric information by restricting the collection, sale, lease, or disclosure of it."²²¹ There are two sections of Texas law that accomplish this. The first is found in Chapter 560 of the Government Code. Section 560.002 states that a "governmental body may not sell, lease, or disclose biometrics unless" the individual consents, disclosure is required or permitted by state or federal law, or the "disclosure is made by a law enforcement agency for a law enforcement purpose."²²² The second section of Texas law that protects the confidentiality of biometric information can be found in Chapter 503 of the Business and Commerce Code. That section limits the circumstances under which a biometric identifier can be captured or collected, as well as the conditions for its disclosure.²²³ Section 503.001(b) states that a person may not use biometrics for a commercial purpose unless the person providing the biometric is informed of its capture beforehand and consents.²²⁴ Furthermore, Section 503.001(c) prohibits the sale, lease, or disclosure of a biometric identifier collected for a commercial purpose except for the identification of an individual in the event of his or her disappearance or death,²²⁵ the completion of a financial transaction authorized by the individual,²²⁶ a purpose required or permitted by state or federal law,²²⁷ or a law enforcement purpose in response to a warrant.²²⁸ Violation of Section 503.001 can result in a penalty of up to \$25,000 per violation.²²⁹

The collection and storage of biometric information by government in Texas is typically done without a warrant or a showing of probable cause. Although warrantless, the collection and storage of this information by Texas government is likely constitutional. As discussed above, the Fourth Amendment to the United States Constitution and Art. 1 Sec. 9 of the Texas Constitution protects "persons, houses, papers, and effects" from unreasonable government searches of places where there is a reasonable expectation of privacy by generally requiring a valid warrant supported by probable cause.²³⁰ ²³¹ The Supreme Court, however, has repeatedly upheld the constitutionality of warrantless government searches conducted incident to arrest or with the

²¹⁸ Dave Lieber, *The Watchdog: Whistleblower blasts DPS for taking fingerprints*, July 13, 2014, <http://www.dallasnews.com/investigations/watchdog/20140712-the-watchdog-whistleblower-blasts-dps-for-taking-fingerprints.ece>

²¹⁹ Tex. Gov't. Code § 560.002(1).

²²⁰ Tex. Bus. & Comm. Code § 503.001(b).

²²¹ Ronald L. Scott, *Protecting Biometric Identifiers*, Aug. 24, 2001,

<https://www.law.uh.edu/healthlaw/perspectives/Privacy/010824Biometrics.html>

²²² Tex. Gov't. Code § 560.002(1)(A)-(C).

²²³ Tex. Bus. & Com. Code, Chapter 503.

²²⁴ Tex. Bus. & Com. Code § 503(b).

²²⁵ Tex. Bus. & Com. Code § 503(c)(1)(A).

²²⁶ Tex. Bus. & Com. Code § 503(c)(1)(B).

²²⁷ Tex. Bus. & Com. Code § 503(c)(1)(C).

²²⁸ Tex. Bus. & Com. Code § 503(c)(1)(D).

²²⁹ Tex. Bus. & Com. Code § 503(d).

²³⁰ U.S. CONST. amend. IV.

²³¹ T.X. Const. art. I, § 9.

consent of the person being searched.²³² The collection of biometric information for driver's licenses, professional licenses, occupational licenses, and the booking of a suspected criminal offense is done consensually or incident to an arrest and is therefore likely constitutional. Furthermore, the Senate Committee on State Affairs is unaware of any instance whereby biometrics have been used by the State of Texas or a political subdivision to monitor the physical location of an individual without a warrant.

Radio Frequency Identification (RFID) is a tracking technology that uses radio waves to identify, track, and monitor physical objects.²³³ It uses radio waves to wirelessly transmit the identity of a unique serial number attached to a chip embedded in an object often carried or possessed by a person.²³⁴ For an RFID chip to transmit its identity, it must be within a certain distance of a "reader," which is the device used to identify the unique serial number attached to the chip.²³⁵ The distance at which a RFID chip or tag can be identified or read by a reader depends on a number of factors, such as the frequency of the radio waves, the size of the RFID chip's antenna, the power output of the reader, and whether the RFID tag is battery-powered.²³⁶ For example, RFID tags with battery power are typically readable from 300 feet, while the tags without battery power, like the ones usually found in smart cards, like the State of Texas employee ID badge, are often readable from only three feet or less.²³⁷ RFID technology has been used to monitor the location of cattle, deer, prison inmates, parolees, warehouse goods, vehicles, and even Texas high school students.²³⁸

This issue gained attention after the media reported the Northside Independent School District in San Antonio was sued for issuing school identification badges with RFID technology.²³⁹ Andrea Hernandez was issued a badge as a high school student in the district, but refused to wear it on religious grounds.²⁴¹ The school district attempted to accommodate Hernandez by removing the chip from her badge.²⁴² The school, however, continued to require Hernandez to wear the chip-less student ID.²⁴³ Not satisfied, Hernandez filed suit against her school.²⁴⁴ Dispensing with the suit, the court ruled against Hernandez, finding the basis for her refusal to wear the identification badge was secular, not religious, given she had previously worn the

²³² *Agnello v. United States*, 269 U.S. 20, 30 (1925).

²³³ RFID Journal, *Frequently Asked Questions*, <http://www.rfidjournal.com/site/faqs#Anchor-What-363> (last visited Dec. 12, 2014).

²³⁴ *Id.*

²³⁵ *Id.*

²³⁶ *Id.*

²³⁷ *Id.*

²³⁸ *Id.*

²³⁹ Bob Owen, *San Antonio schools' test of student ID 'locator' chips faces religious suit*, The Dallas Morning News, November 27, 2012, <http://www.dallasnews.com/news/education/headlines/20121127-lawsuit-targets-san-antonio-schools-student-id-locator-chips-on-religious-grounds.ece>

²⁴⁰ At least five other independent school districts were also using RFID technology to track student attendance, including Austin ISD, Kellar ISD, Manor ISD, Spring ISD, and Santa Fe ISD.

²⁴¹ Natasha Lennard, *Judge: Texas school can force student to wear RFID badge*, Salon, January 9, 2013, http://www.salon.com/2013/01/09/judge_texas_school_can_force_student_to_wear_rfid_badge/

²⁴² *Id.*

²⁴³ *Id.*

²⁴⁴ *Id.*

identification badge without complaint and that the school had offered to remove the RFID chip.²⁴⁵

Perhaps not surprisingly, the use of RFID chips by public schools was the subject of several pieces of legislation during the 83rd Regular Session of the Texas Legislature. House Bill 101 was one of those pieces of legislation. Filed on November 12, 2012, it required a school district's board of trustees to approve of the use of RFID technology and would have allowed a student to opt-out of using the technology upon written notice from the parent or guardian of the student.²⁴⁶ House Bill 101 was reported from the House Committee on Education and was sent to the House Committee on Calendars, where it remained until session ended on May 27, 2013.²⁴⁷ A bill filed in the Senate also addressed this issue, but in a different way. Senate Bill 173 was filed on January 11, 2013, and would have flatly prohibited schools from using RFID technology for the purpose of tracking or collecting information on public school students.²⁴⁸ The bill was referred to the Senate Committee on Education, but did not receive a hearing.²⁴⁹ After filing Senate Bill 173, bill author Senator Craig Estes captured the concern of many in the legislature regarding the use of RFID technology to monitor the location of students:

*I do not want our children and grandchildren to grow up in a world where this type of intrusive, big-brother surveillance is considered normal. This is the same type of technology used to track cattle, so it's disturbing to me that we are now seeing government use that same surveillance technology to track and monitor our young citizens. Using RFID tags to track children is a perfect example of big-government run amuck. It's time for legislators to step in and protect our citizens' privacy.*²⁵⁰

Texas is not the only state where legislation has recently been filed to regulate the use of RFID technology in public schools. In Missouri, the legislature last month overrode the governor's veto of Senate Bill 523, which states, "no school district shall require a student to use an identification device that uses radio frequency identification technology, or similar technology, to identify the student, transmit information regarding the student, or monitor or track the location of the student."²⁵¹ Moreover, an Oregon law passed in June 2013 directs the State Board of Education to "adopt standards for a school district board to incorporate into any policy that requires students to wear, carry or use item with radio frequency identification device for purpose of locating or tracking student or taking attendance."²⁵²

²⁴⁵ Natasha Lennard, *Judge: Texas school can force student to wear RFID badge*, Salon, January 9, 2013, http://www.salon.com/2013/01/09/judge_texas_school_can_force_student_to_wear_rfid_badge/

²⁴⁶ H.B. 101, 83rd Leg., Regular Sess. (Tex. 2013).

²⁴⁷ *H.B. 101 History*, Texas Legislature Online, <http://www.capitol.state.tx.us/BillLookup/History.aspx?LegSess=83R&Bill=HB101> (last visited Dec. 12, 2014).

²⁴⁸ S.B. 173, 83rd Leg., Regular Sess. (Tex. 2013).

²⁴⁹ *S.B. 173 History*, Texas Legislature Online, <http://www.capitol.state.tx.us/BillLookup/History.aspx?LegSess=83R&Bill=SB173> (last visited Dec. 12, 2014).

²⁵⁰ Chris Agee, *Estes bill targets RFID technology in schools*, Mineral Well Index, Jan. 16, 2013, http://www.mineralwellsindex.com/news/local_news/estes-bill-targets-rfid-technology-in-schools/article_8c1a1c18-3a30-5508-b36f-a2ec5f6d3f81.html

²⁵¹ S.B. 523, 97th Gen. Ass., 2nd Reg. Sess. (Mo. 2014) (enacted).

²⁵² Or. Rev. Stat. § 339.890(1).

Whether in Missouri, Oregon, or Texas, the use of RFID technology requires a chip (or a tag) and a reader. The technology does not function without these components. This practical reality places legal, logistical, and financial constraints on the use of RFID technology to monitor the physical location of individuals. First, the logistics of using this technology to track people wherever they go would require the placement of readers at intervals of no bigger than 100-300 feet while forcing each monitored person to carry or wear an RFID tag during the required monitoring times. Second, the cost of using RFID technology to monitor the physical location of people within a large area could be tremendous. Take the state of Texas for example, which is the second largest state in the United States at 268,581 square miles. Placed at intervals of 100 feet, millions of readers would likely be needed to cover the entire state. At an estimated cost of \$500-2,000 per reader,²⁵³ the expense of installing RFID readers across the entire state could be larger than the United States national debt. Lastly, even if the logistical and financial obstacles were overcome, the Supreme Court has said a person has a reasonable expectation of privacy in their body that the Fourth Amendment protects from unreasonable government searches, such as requiring a person to carry an RFID chip around.²⁵⁴ This likely would require that the government obtain a valid search warrant for or the voluntary consent of the vast majority of individuals to be monitored.

Due to the legal, logistical, and financial obstacles involved, government use of RFID technology in Texas is generally limited to swiping an employee identification badges at the entrances of government buildings, and the scanning of a TxTag at certain locations along tolled highways.²⁵⁵ In the vast majority of cases, if not all of them, a person freely chooses to work as an employee for the state of Texas or travel on a tolled Texas highway using a TxTag. Thus, similar to government collection of biometrics, the use of RFID technology, while warrantless, is likely nonetheless constitutional because its use to monitor physical location is done with the consent of those being monitored. House Bill 3199 from the 83rd Regular Session of the Texas Legislature would have expanded the use of RFID technology in Texas to driver licenses, which do not currently contain an RFID chip.²⁵⁶ The bill required the Texas Department of Public Safety to issue "secure driver licenses" with an "integrated circuit chip" to certain groups of people, such as "emergency personnel" and an "applicant for the provision of state and federal government program benefits."²⁵⁷ House Bill 3199 was considered in a public hearing of the House Committee on Homeland Security and Public Safety on May 2, 2013, and was left pending until session ended on May 27, 2013.²⁵⁸

²⁵³ RFID Journal, *How much do RFID readers cost today?*, <http://www.rfidjournal.com/faq/show?86> (last visited on Dec. 12, 2014).

²⁵⁴ *Schmerber v. California*, 384 U.S. 757, 769-70 (1966).

²⁵⁵ TxTag is the name of the RFID device affixed to the windshield of a vehicle that is linked in an financial account used to pay toll fees to the Texas Department of Transportation for the use of a tolled highway.

²⁵⁶ H.B. 3199, 83rd Leg., Regular Sess. (Tex. 2013).

²⁵⁷ *Id.*

²⁵⁸ *H.B. 3199 History*, Texas Legislature Online, <http://www.capitol.state.tx.us/BillLookup/History.aspx?LegSess=83R&Bill=HB3199> (last visited Dec. 12, 2014).

At least sixteen states, including Texas, have laws related to the use of RFID technology.²⁵⁹ There are generally three types of substantive state RFID laws. The first prohibits the forced implantation of a RFID microchip. According to the National Conference of State Legislatures, only six states have this type of law: California, Georgia, North Dakota, Oklahoma, Virginia, and Wisconsin.²⁶⁰ Legislators in Colorado, Florida, and Ohio all tried to pass similar legislation in 2007, but were unsuccessful.²⁶¹ The second type of state RFID law proscribes "skimming," which is the unauthorized reading and duplication of the information contained by a RFID chip often to commit identity or credit card theft.²⁶² States that ban skimming include Alabama, California, Illinois, Nevada, and Washington.²⁶³ The last type of RFID-related state law regulates the use of RFID technology in driver's licenses.²⁶⁴ For example, Texas requires the encryption of RFID technology if used in a driver's license.²⁶⁵ Arkansas, Michigan, Minnesota, Vermont, Virginia, and Washington also have laws relating to the use of RFID technology in drivers licenses or vehicles.²⁶⁶

Facial recognition is an increasingly accurate biometric identification technique that cross references an image of a person's face with a facial database to determine the identity of that person.²⁶⁷ A Minnesota-based company, Identix, has developed a software application called FaceIt that "can pick someone's face out of a crowd, extract the face from the rest of the scene and compare it to a database of stored images."²⁶⁸ Software like this is based on the ability to measure the various features of the face, such as the distance between the eyes, width of the nose, depth of the eye sockets, contours of the cheekbones, and length of the jaw line.²⁶⁹ Once measured, those features are used to create a digital map of a person's face.²⁷⁰ There are approximately 80 points on each of these maps called "nodal points," which are used to create a "numerical code" for a particular face called a "faceprint."²⁷¹ A faceprint is then cross-referenced with a facial database to search for a "match" in order to determine the identity of a particular person.²⁷²

²⁵⁹ National Conference of State Legislatures, *State Statutes Relating to Radio Frequency Identification (RFID) and Privacy*, Dec. 13, 2013, <http://www.ncsl.org/research/telecommunications-and-information-technology/radio-frequency-identification-rfid-privacy-laws.aspx>

²⁶⁰ *Id.*

²⁶¹ *Against RFID in Schools, Laws and Legislation*, <http://rfidinschools.com/laws-legislation/> (last visited Dec. 12, 2014).

²⁶² National Conference of State Legislatures, *State Statutes Relating to Radio Frequency Identification (RFID) and Privacy*, Dec. 13, 2013, <http://www.ncsl.org/research/telecommunications-and-information-technology/radio-frequency-identification-rfid-privacy-laws.aspx>

²⁶³ *Id.*

²⁶⁴ *Id.*

²⁶⁵ *Id.*

²⁶⁶ *Id.*

²⁶⁷ Kevin Bonsor and Ryan Johnson, *How Facial Recognition Systems Work*, HowStuffWorks.com, <http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>

²⁶⁸ *Id.*

²⁶⁹ *Id.*

²⁷⁰ *Id.*

²⁷¹ *Id.*

²⁷² *Id.*

While facial recognition still generally works this way, the technology has advanced from two-dimensional to three-dimensional imagery.²⁷³ In the beginning, facial recognition software determined the identity of a person by comparing a two-dimensional image to another two-dimensional image in a database.²⁷⁴ Frustratingly, the use of two-dimensional images were often ineffective or inaccurate because the limitations of two-dimensional technology required the captured image to have very nearly the same angle, light, and facial expression as the image in the database.²⁷⁵ Since most captured images used for facial recognition are not taken in controlled environments, most of them were not similar enough to the images of the same person stored in facial databases.²⁷⁶ Necessarily, this caused a high rate of failure within two-dimensional facial recognition systems.²⁷⁷ There is, however, a "newly-emerging trend in facial recognition software [that] uses a three-dimensional model..."²⁷⁸ Developers claim that the use of three-dimensional images is more accurate because the technology better captures the distinctive features of the face, such as the facial curves of the eye socket, nose, and chin, which is crucial to the creation of the faceprint and thus the matching process.²⁷⁹ Additionally, three-dimensional facial recognition is not affected by variances in lighting or angle, and can be used in darkness and at angles upwards of 90 degrees.²⁸⁰

Over the years, facial recognition has been used by many different organizations for many different purposes. The Federal Bureau of Investigation ("FBI") recently launched its new facial recognition system, Next Generation Identification ("NGI"), to prevent, solve, and prosecute crime.²⁸¹ The NGI database combines all forms of biometric data, such as fingerprints, retina scans, and faceprints, into a file for each individual for which there is at least one data point and links that file to personal and biographic data, such as a person's name, home address, immigration status, age, and race.²⁸² According to the Electronic Frontier Foundation, the NGI database will have at least 100 million fingerprints and 52 million facial records by 2015, and is being "shared with approximately 18,000 tribal, state, and local law enforcement agencies across the United States."²⁸³ States sharing and accessing face data with the FBI through the NGI database include Michigan, Maryland, and Hawaii, but not Texas.²⁸⁴ In Massachusetts, the Boston Police Department used facial recognition software to capture photos of people attending

²⁷³ Kevin Bonsor and Ryan Johnson, *How Facial Recognition Systems Work*, HowStuffWorks.com, <http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>.

²⁷⁴ *Id.*

²⁷⁵ *Id.*

²⁷⁶ *Id.*

²⁷⁷ *Id.*

²⁷⁸ *Id.*

²⁷⁹ *Id.*

²⁸⁰ *Id.*

²⁸¹ Jose Pagliery, *FBI launches a face recognition system*, Sept. 16, 2014, <http://money.cnn.com/2014/09/16/technology/security/fbi-facial-recognition/>

²⁸² Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, April 14, 2014, <https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year>

²⁸³ *Id.*

²⁸⁴ *Id.*

local music festivals.²⁸⁵ The city of Chicago has 25,000 surveillance cameras connected to facial recognition software which, in 2013, the Chicago Police Department used to identify and arrest a suspected purse-snatcher.²⁸⁶ The Tampa Bay Police Department in 2001 installed police cameras equipped with facial recognition technology in their Ybor City nightlife district in an attempt to reduce crime in the area.²⁸⁷ The system, however, was scrapped two years later because "people in the area were seen wearing masks and making obscene gestures, prohibiting the cameras from getting a clear enough shot to identify anyone."²⁸⁸ In the private sector, Facebook has developed a facial recognition program called *DeepFace* that determines the identity of people in the millions of images uploaded to its website with 97.25 percent accuracy, which is a mere quarter percentage point lower than the accuracy rate of a human brain.²⁸⁹ Additionally, a Google Glass application known as *NameTag* "can scan faces and try to find a match in a compiled database of over 2.5 million faces."²⁹⁰

In response to government and commercial use of facial recognition technology, "there's an increasing amount of discussion and experimentation on how to fool and spoof automatic visual recognition systems" to conceal a person's identity.²⁹¹ The simplest and most widespread technique "is to wear a mask, hoodie, bandana or similar face covering."²⁹² For example, Chicago-based artist Leo Selvaggio has created a "personal surveillance identity prosthetic" or "privacy mask" out of his own image to "shield people's identities – from everyday pedestrians to active protesters – whether they're in a public urban space or just shooting selfies on Facebook."²⁹³ Another example is the adoption of the Guy Fawkes mask, which both protects the wearer's identity while signaling participation in a shared cause.²⁹⁴ In addition to wearing a mask, people have turned to a technique called "CV dazzle" to protect their identity from facial recognition technology.²⁹⁵ CV dazzle has been called "anti-surveillance camouflage for your face" and described as "a drastic technique to throw the machines off your trail."²⁹⁶ It involves painting patterns of shapes on the face, which distort and disrupt the ability of facial recognition

²⁸⁵ Giuseppe Macri, *Boston PD Tested Facial Recognition Software By Recording Every Face At Local Music Festivals*, The Daily Caller, Aug. 18, 2014, <http://dailycaller.com/2014/08/18/boston-pd-tested-facial-recognition-software-by-recording-every-face-at-local-music-festivals/>

²⁸⁶ Mark Wilson, *Subversive Mask Fools Surveillance Cameras*, Fast Company, May 8, 2014, <http://www.fastcodesign.com/3030206/subversive-mask-fools-surveillance-cameras>

²⁸⁷ Kevin Bonsor and Ryan Johnson, *How Facial Recognition Systems Work*, HowStuffWorks.com, <http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>

²⁸⁸ *Id.*

²⁸⁹ Luke Dormehl, *Facial recognition: is the technology taking away your identity?*, The Guardian, May 4, 2014, <http://www.theguardian.com/technology/2014/may/04/facial-recognition-technology-identity-tesco-ethical-issues>

²⁹⁰ Raymond Wong, *Real-time Google Glass app can ID people using facial recognition*, Dvice, Feb 6, 2014, <http://www.dvice.com/2014-2-6/real-time-google-glass-app-can-id-people-using-facial-recognition>

²⁹¹ Sameer Padania, *How to Defend Yourself Against Facial Recognition Technology*, PBS, June 18, 2012, <http://www.pbs.org/mediashift/2012/06/how-to-defend-yourself-against-facial-recognition-technology170/>

²⁹² *Id.*

²⁹³ Mark Wilson, *Subversive Mask Fools Surveillance Cameras*, Fast Company, May 8, 2014, <http://www.fastcodesign.com/3030206/subversive-mask-fools-surveillance-cameras>

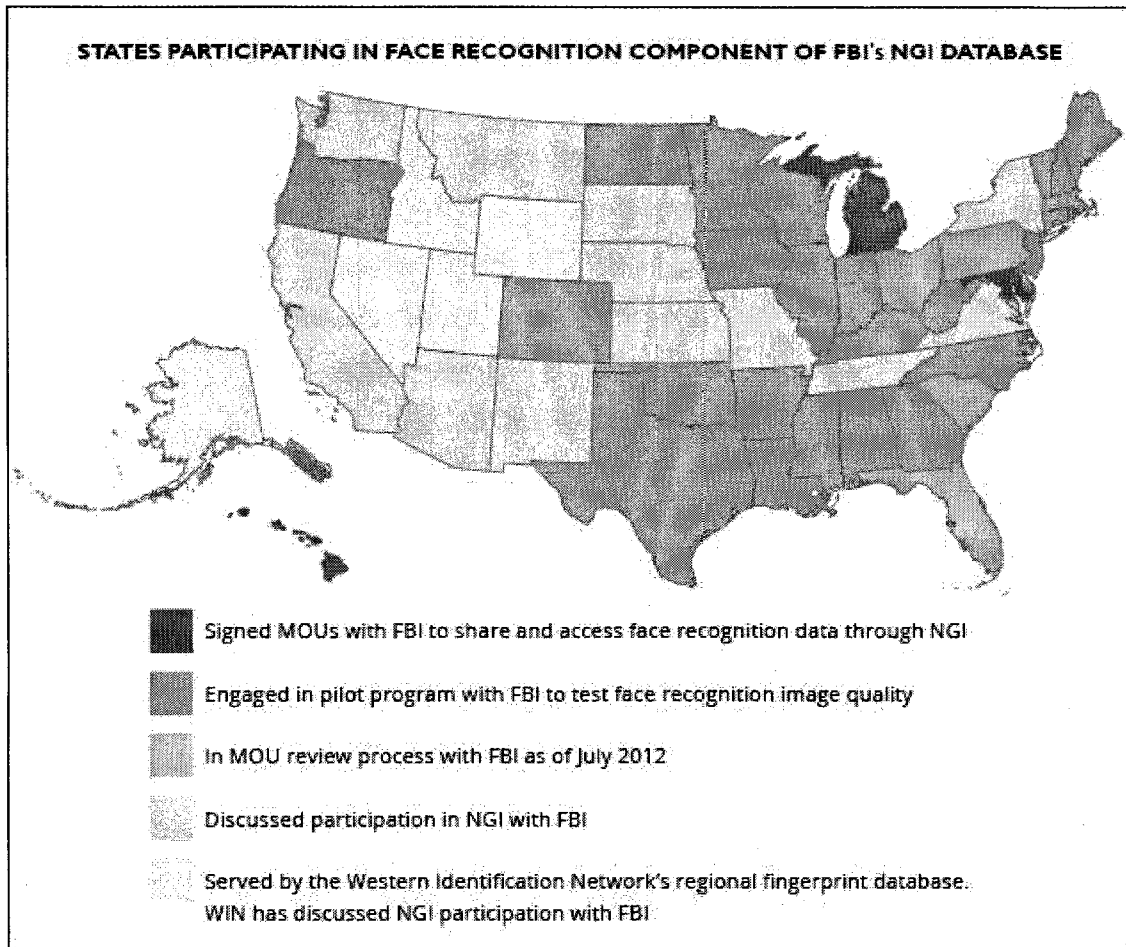
²⁹⁴ *Id.*

²⁹⁵ Robinson Meyer, *Anti-Surveillance Camouflage for Your Face*, The Atlantic, July 24, 2014, <http://www.theatlantic.com/features/archive/2014/07/makeup/374929/>

²⁹⁶ *Id.*

software to accurately locate and measure nodal points, throwing off the creation of the faceprint and in turn the matching process.²⁹⁷

The idea behind CV dazzle is simple. Facial recognition algorithms look for certain patterns when they analyze images: patterns of light and dark in the cheekbones, or the way color is distributed on the nose bridge—a baseline amount of symmetry. These hallmarks all betray the uniqueness of a human visage. If you obstruct them, the algorithm can't separate a face from any other swath of pixels.²⁹⁸



Source: Electronic Frontier Foundation

Essentially, CV dazzle, "confounds computers with color and light."²⁹⁹ Ironically, however, it has been reported that while CV dazzle "makes you invisible to computers" it also "makes you glaringly obvious to other humans," perhaps undermining any privacy benefits.³⁰⁰ In addition to these grassroots efforts, there have been legislative efforts in Texas to regulate the use of facial

²⁹⁷ Robinson Meyer, *Anti-Surveillance Camouflage for Your Face*, The Atlantic, July 24, 2014, <http://www.theatlantic.com/features/archive/2014/07/makeup/374929/>

²⁹⁸ *Id.*

²⁹⁹ *Id.*

³⁰⁰ *Id.*

recognition technology.³⁰¹ During the 83rd Regular Session of the Texas Legislature, Senate Bill 1052 was successfully amended by Representative Scott Sanford to prohibit a retail establishment from using facial recognition technology for any purpose.³⁰²

Facial recognition technology has existed since the 1960s when "scientists began work on using the computer to recognize human faces."³⁰³ Yet, there are no specific federal laws governing the use of facial recognition technology.³⁰⁴ Jennifer Lynch, an attorney with the Electronic Frontier Foundation, attributes the lack of public policy on facial recognition to the fact that "many Americans don't even realize...they're already in a facial recognition database," likely because the technology "allows for covert, remote and mass capture of identification and images."³⁰⁵ Some Americans are aware, however, and at least one United States Senator has called for limits on this technology. Senator Al Franken (D-MN) believes a person has a "fundamental right to control their private information"³⁰⁶ because unlike a password or a credit card "you can't change your fingerprint, and you can't change your face, unless you go through a great deal of trouble."³⁰⁷ Franken has called on the FBI to limit its use of facial recognition technology because "he's concerned that law enforcement agencies will use the technology to track people at legal protests and other gatherings."³⁰⁸ The U.S. Senator for Minnesota has also called on Facebook to make use of its facial recognition technology or "tag suggestion" feature opt-in, instead of opt-out.³⁰⁹ Both the FBI and Facebook have, however, mostly ignored those calls and are moving ahead with the use of facial recognition technology.³¹⁰

An example of where the calls of privacy advocates were not ignored can be found in Ohio, where a facial recognition system launched last year.³¹¹ Initially, the system allowed approximately 30,000 law enforcement officers to capture an image of an unknown person and compare it to a database of 23 million Ohio driver license photos and mug shots to establish a match.³¹² After its release, however, the American Civil Liberties Union (ACLU) voiced

³⁰¹ Tex. House Journal, 83rd Leg., Regular Sess., 20 May 2013 (pg. 3846).

³⁰² *Id.*

³⁰³ Kevin Bonsor and Ryan Johnson, *How Facial Recognition Systems Work*, HowStuffWorks.com, <http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm>

³⁰⁴ Natasha Singer, *Never Forgetting a Face*, The N.Y. Times, May 17, 2014, http://www.nytimes.com/2014/05/18/technology/never-forgetting-a-face.html?_r=0

³⁰⁵ Senate Committee on the Judiciary Subcommittee on Privacy, Technology, and the Law hearing, July 18, 2012 (Written testimony of Jennifer Lynch, Electronic Frontier Foundation).

³⁰⁶ Grant Gross, *Regulation of facial recognition may be needed, US senator says*, ComputerWorld, July 18, 2012, <http://www.computerworld.com/article/2506105/technology-law-regulation/regulation-of-facial-recognition-may-be-needed--us-senator-says.html>

³⁰⁷ T.C. Sottek, *Senator Al Franken grills FBI, Facebook, and others on facial recognition technology*, The Verge, July 18, 2012, <http://www.theverge.com/2012/7/18/3167864/senator-al-franken-fbi-facebook-facial-recognition-hearing>

³⁰⁸ Grant Gross, *Regulation of facial recognition may be needed, US senator says*, ComputerWorld, July 18, 2012, <http://www.computerworld.com/article/2506105/technology-law-regulation/regulation-of-facial-recognition-may-be-needed--us-senator-says.html>

³⁰⁹ *Id.*

³¹⁰ *Id.*

³¹¹ J.D. Tuccille, *30,000 Cops Can Access Ohio's Facial Recognition Database Without Oversight, Says Report*, Reason.com, Sept. 23, 2013, <http://reason.com/blog/2013/09/23/30000-cops-can-access-ohios-facial-recog>

³¹² *Id.*

concerns that giving 30,000 law enforcement officers access to the system would, in time, lead to abuse and privacy violations.³¹³ This prompted Ohio Attorney General Mike DeWine to limit access to the system.³¹⁴ Now, fewer than 6,000 law enforcement officers have access to facial recognition technology in the state.³¹⁵

Recommendation

There are no further necessary limits on the warrantless search or seizure of digital data because the search or seizure of that type of information now requires a warrant pursuant to federal or state law. Necessary limits, however, may need to be placed on the warrantless search of geolocational data, especially historic cell-site location-data. In deciding and determining what, if any, limits are necessary, the Legislature must continue to balance the needs of Texas law enforcement and the reasonable privacy expectations of Texans.

There are numerous provisions in Texas law that protect against non-consented audio and video recordings, whether or not collected by private handheld and wearable mobile devices or not. However, if the Legislature decides to establish additional protections, it must balance the interest of technological innovation that, among other applications, may ease the capture of non-consented recordings with the need to protect Texans' reasonable expectations of privacy.

Lastly, the Legislature should continue to monitor government use of biometrics, radio frequency identification, and facial recognition to track the physical location of individuals and, if necessary, find a balance that preserves a reasonable expectation of privacy and the appropriate use of those technologies.

Charge No. 3

Review the types and scope of personal data collected by governmental and commercial entities and consider methods to minimize the government's collection of data on its citizens. The study should include: (1) whether sufficient protections exist for DNA samples and information, including whether there should be a prohibition on the creation of DNA databases, except for felons and sex offenders; (2) methods to protect the privacy of gun owners from aggregated purchasing pattern tracking; (3) mechanisms to ensure that private health care information is properly protected; and (4) ways to ensure that previously anonymous data is not improperly re-identified and marketed. Examine related measures proposed or passed in other states.

Whether sufficient protections exist for DNA samples and information, including whether there should be a prohibition on the creation of DNA databases, except for felons and sex offenders.

³¹³ Kade Crockford, *Ready, fire, aim: Ohio officials implement statewide face recognition program without a whiff of public debate*, American Civil Liberties Union, Sept. 3, 2013, <https://www.aclu.org/blog/technology-and-liberty-national-security/ready-fire-aim-ohio-officials-implement-statewide-face>

³¹⁴ M.L. Schultze, *DeWine significantly cuts access to Ohio facial recognition software*, WKSU, Aug. 1, 2014, <http://www.wksu.org/news/story/39975>

³¹⁵ *Id.*

Deoxyribonucleic acid, or DNA, was first observed by Swiss biochemist Friedrich Miescher in 1869 when he extracted it from the pus of discarded surgical bandages.³¹⁶ Since then, scientific research has determined that DNA is a replicative, hereditary double helix molecule responsible for protein synthesis that is found in the nucleus of each cell of an organism.³¹⁷ It serves as the instruction manual and blueprint for every human.³¹⁸ Although some DNA distinguishes one person from everyone else, approximately 99.9 percent of human DNA is the same for all people.³¹⁹ This leaves only about one-tenth of one percent, or approximately 3 million pairs of DNA, that are distinctive to each person.³²⁰ Thus, it is nearly impossible for two people to have the exact same DNA.³²¹ Consequently, it can be analyzed to determine the identity of the person to whom it belongs with tremendous precision and accuracy. This is the primary reason DNA has numerous applications in today's world. For example, DNA can be analyzed to identify the biological father of a child or to ascertain the identity of skeletal remains.³²² DNA samples are also regularly used to investigate human populations, clarify history, and study genetic disorders like Down syndrome and sickle-cell disease.³²³ However, due to the popularity of television shows about crime scene investigation, the most well-known application of DNA analysis is to solve crime.³²⁴

The use of DNA to solve crime, called DNA profiling, was pioneered by Alec Jeffreys at the University of Leicester in Great Britain during the 1980s.³²⁵ The process begins with a sample of person's DNA, such as a bloody weapon, sweaty shirt, or snotty facial tissue.³²⁶ ³²⁷ Typically called a "reference sample," the DNA is then analyzed to create a person's DNA profile.³²⁸ There are several different techniques used to analyze DNA, such as restriction fragment length polymorphism (RFLP) analysis, polymerase chain reaction (PCR) analysis, or short tandem repeats (STR) analysis.³²⁹ The Federal Bureau of Investigation (FBI) uses the STR method, which if identical twins are excluded, reduces the likelihood any two people will have the exact same DNA profile to one in a billion.³³⁰ Ideally, the last step of the profiling process compares a sample of the DNA collected at the crime scene to a sample provided by a suspect for the

³¹⁶ Dahm, R: Friedrich Miescher and the discovery of DNA. *Developmental Biology*, 2005, Vol. 278(2), p. 274-288.

³¹⁷ Genetics Home Reference: Your Guide to Understanding Genetic Conditions, *What is DNA?*, <http://ghr.nlm.nih.gov/handbook/basics/dna> (last visited Dec. 8, 2014).

³¹⁸ *Id.*

³¹⁹ *Id.*

³²⁰ *Id.*

³²¹ Monozygotic ("identical") twins have identical DNA, but represent only 0.2 percent of the population.

³²² DNA Interactive, *Applications*, <http://www.dnai.org/d/> (last visited Dec. 8, 2014).

³²³ *Id.*

³²⁴ William Harris, *How DNA Evidence Works*, HowStuffworks.com, <http://science.howstuffworks.com/life/genetic/dna-evidence.htm>

³²⁵ Adrian Lee, *The godfather of DNA fingerprints: How Alec Jeffreys revolutionized solving crime*, *Express* (Sept. 6, 2014, 9:37 AM), <http://www.express.co.uk/life-style/life/507693/The-godfather-of-DNA-30-years-Alec-Jeffreys-revolutionized-crime-fighting>

³²⁶ Hair, dandruff, semen, skin, and finger nails are also commonly used to obtain a DNA sample.

³²⁷ William Harris, *How DNA Evidence Works*, HowStuffWorks.com <http://science.howstuffworks.com/life/genetic/dna-evidence.htm>

³²⁸ *Id.*

³²⁹ *Id.*

³³⁰ *Id.*

crime.³³¹ This comparison often excludes (*i.e.*, eliminates suspicion) or continues to include (*i.e.*, reaffirms suspicion) that person as a suspect.³³²

Unfortunately, however, there is not always a suspect.³³³ In those cases, a DNA sample is compared to a DNA profile digitized and electronically stored in a database maintained by local, state, or federal law enforcement agencies.³³⁴ One such database is the National DNA Index System, or NDIS.³³⁵ Authorized by the DNA Identification Act of 1994, the NDIS contains "DNA profiles contributed by federal, state, and local participating forensic laboratories."³³⁶ All fifty states, the District of Columbia, and the federal government participate in NDIS,³³⁷ which as of August 2014, contained more than 11 million offender profiles, nearly 2 million arrestee profiles, and just short of 600,000 forensic profiles.³³⁸

As a participant, Texas must meet certain laboratory standards, limit access to DNA records in accordance with federal law, and maintain its own DNA database.³³⁹ The Texas State DNA Index System (SDIS) was created by House Bill 40, which passed during 74th Regular Session of the Texas Legislature in 1995. Since its passage, Texas law has required the Department of Public Safety (DPS) to "record DNA data" and operate a "computerized database that serves as the central depository in the state for DNA records."³⁴⁰ The database classifies, matches, and stores the results of DNA analysis.³⁴¹ In addition, it is compatible with the Combined DNA Index System (CODIS),³⁴² which is a software program developed and used by the FBI that links NDIS, the SDIS from each participating state, and local DNA databases.³⁴³ CODIS allows a law enforcement officer to comprehensively search DNA profiles from crime scene evidence against DNA profiles from other crime scenes and from convicted offenders and arrestees.³⁴⁴

³³¹ William Harris, *How DNA Evidence Works*, HowStuffWorks.com
<http://science.howstuffworks.com/life/genetic/dna-evidence.htm>

³³² *Id.*

³³³ *Id.*

³³⁴ *Id.*

³³⁵ *Id.*

³³⁶ *Frequently Asked Questions (FAQs) on the CODIS Program and the National DNA Index System*, Federal Bureau of Investigation, <http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-fact-sheet> (last visited Dec. 8, 2014).

³³⁷ *Id.*

³³⁸ *CODIS—NDIS Statistics*, Federal Bureau of Investigation, <http://www.fbi.gov/about-us/lab/biometric-analysis/codis/ndis-statistics> (last visited Dec. 8, 2014).

³³⁹ *Frequently Asked Questions (FAQs) on the CODIS Program and the National DNA Index System*, Federal Bureau of Investigation, <http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-fact-sheet> (last visited Dec. 8, 2014).

³⁴⁰ Tex. Gov't. Code § 411.142.

³⁴¹³⁴¹ *Statewide CODIS DNA Database Program Overview*, Department of Public Safety
<https://www.txdps.state.tx.us/CrimeLaboratory/CODIS/> (last visited on Dec. 8, 2014).

³⁴² Tex. Gov't. Code § 411.142(f).

³⁴³ *Frequently Asked Questions (FAQs) on the CODIS Program and the National DNA Index System*, Federal Bureau of Investigation, <http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-fact-sheet> (last visited Dec. 8, 2014).

³⁴⁴ *Id.*

Texas law does not, however, generally require that every person in the state submit a DNA sample for analysis and storage in the CODIS, NDIS, or SDIS database. Instead, Texas law limits who is required to submit a sample, the purposes for which the sample may be used, and the laboratories in which the samples can be processed.³⁴⁵ Under Texas law, a person is not required to submit a DNA sample for analysis and storage in the SDIS database, unless:

- The person has been convicted of a felony and consequently sent to a state prison;³⁴⁶
- The person is older than the age of 18 (i.e., an adult) and has been convicted of a felony and placed on probation;³⁴⁷
- The person is younger than the age of 18 (i.e., a juvenile) and has been convicted of a serious or violent felony, such as assault with a deadly weapon, and placed on probation;³⁴⁸
- The person has been formally charged with a felony, such as sexual assault, compelling prostitution, or possession of child pornography, listed by Section 411.1471 of the Government Code;³⁴⁹
- The person has been convicted of a sexual offense and is a registered sexual offender;³⁵⁰
- The person has been convicted of a misdemeanor sexual offense, such as public lewdness or indecent exposure;³⁵¹ or
- The person has been arrested for a certain felony offense while on deferred adjudication for a certain felony offense.³⁵²

In these limited situations – involving arrest, indictment, or conviction for a sexual, violent, or serious felony – a person is required to submit a sample for analysis and storage under Texas law.³⁵³ If a person refuses to submit a sample, a criminal justice agency is authorized by Section 411.148(h) of the Government Code to use force if necessary to collect the sample, which is typically done by drawing blood or swabbing the inside of a person's cheek. In criminal cases, the law restricts the purposes for which these samples can be used to the investigation of criminal offenses, exclusion or identification of suspects or offenders, or the legal defense or prosecution of a case in a court of law.³⁵⁴ Furthermore, the law requires that DNA samples be processed in a laboratory accredited by DPS for having met or exceeded the standards of the American Society of Crime Lab Directors Lab Accreditation Board.³⁵⁵

³⁴⁵ Tex. Gov't. Code, Chapter 411, Subchapter G.

³⁴⁶ Tex. Gov't. Code § 411.148(a)(1)(B).

³⁴⁷ Tex. Code of Criminal Procedure Art. 42.12 § 11(j).

³⁴⁸ Tex. Gov't. Code § 411.148(a)(2).

³⁴⁹ Tex. Gov't. Code § 411.1471(a)(1)(A)-(K).

³⁵⁰ Tex. Gov't. Code § 411.1473(b).

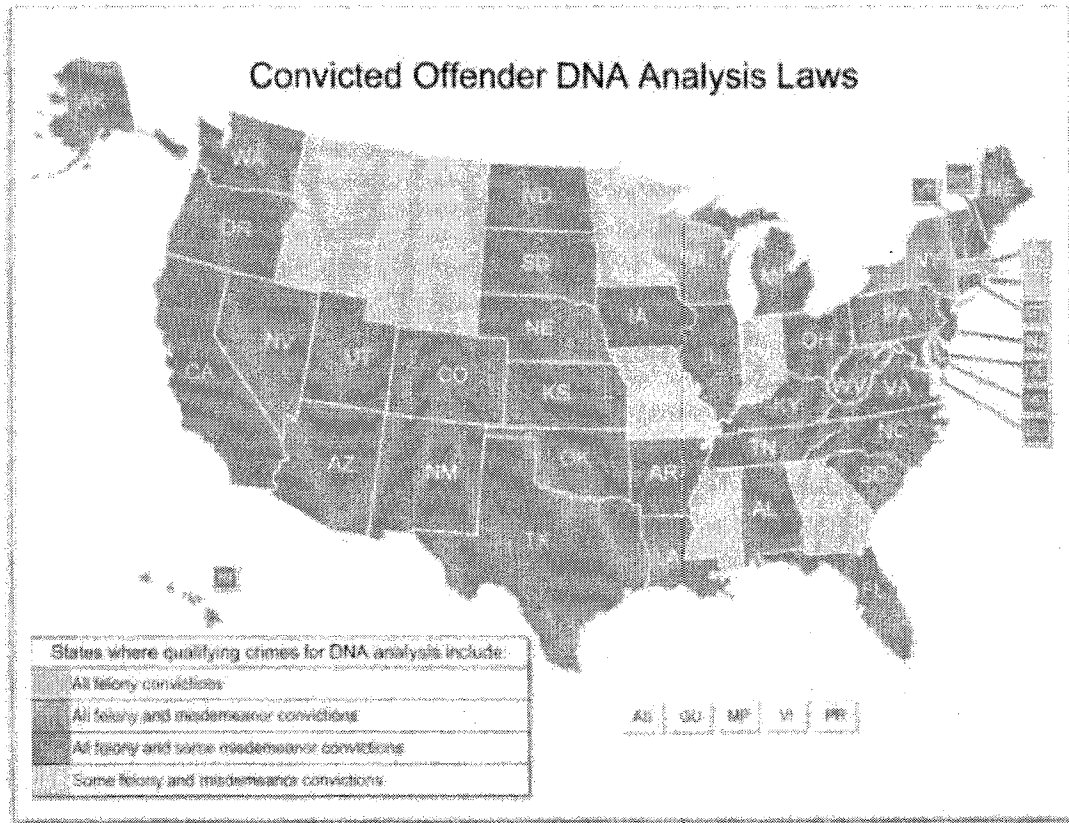
³⁵¹ Tex. Gov't. Code § 411.1471(a)(3).

³⁵² Tex. Gov't. Code § 411.1471(a)(2).

³⁵³ Tex. Gov't. Code, Chapter 411, Subchapter G.

³⁵⁴ Tex. Gov't. Code § 411.143(b).

³⁵⁵ Tex. Gov't. Code § 411.0205.



Source: National Conference of State Legislatures

As of October 2014, there were more than 736,000 offender profiles in the Texas DNA database.³⁵⁶ Texas law protects these profiles in several ways. First, the name of a person and other personal identifying information are not allowed to be stored in CODIS.³⁵⁷ ³⁵⁸ Similarly, the collection, analysis, or storage of information in the database to assess physical traits or predisposition for disease is generally prohibited.³⁵⁹ Third, the law restricts the release of DNA records, analysis, and samples to certain people for certain purposes.³⁶⁰ Section 411.147 of the Government Code limits disclosure to a criminal justice agency for a criminal justice or law enforcement identification purpose,³⁶¹ a court of law for a judicial proceeding,³⁶² a defendant for their criminal defense,³⁶³ a person as required by federal law,³⁶⁴ or a person for a purpose listed in Section 411.143 of the Government Code, such as recovering or identifying human remains after a disaster or identifying a missing person.³⁶⁵ Relatedly, records held in the Texas DNA

³⁵⁶ CODIS—NDIS Statistics, Federal Bureau of Investigation, <http://www.fbi.gov/about-us/lab/biometric-analysis/codis/ndis-statistics/#Texas> (last visited Dec. 8, 2014).

³⁵⁷ The CODIS system, however, may contain a reference number that when matched with the same reference number in another information system may provide personal identifying information, such as a person's name.

³⁵⁸ Tex. Gov't. Code § 411.143(e).

³⁵⁹ Tex. Gov't. Code § 411.143(d).

³⁶⁰ Tex. Gov't. Code § 411.147.

³⁶¹ Tex. Gov't. Code § 411.147(c)(1).

³⁶² Tex. Gov't. Code § 411.147(c)(2).

³⁶³ Tex. Gov't. Code § 411.147(c)(3).

³⁶⁴ Tex. Gov't. Code § 411.147(c)(4)(B).

³⁶⁵ Tex. Gov't. Code § 411.147(c)(4)(A).

database are confidential and not subject to disclosure under the Texas Public Information Act.³⁶⁶ The punishment for knowingly disclosing a DNA record to a recipient not authorized by the law is a state jail felony and considered official misconduct under Section 411.153 of the Government Code.³⁶⁷ Furthermore, a court is required by law to order the destruction of a DNA specimen collected from a person indicted or arrested for a crime, if that person is subsequently acquitted or the case dismissed. Lastly, a court may expunge an adult's DNA record by using the standard procedures for the expunction of criminal records or a juvenile's DNA record by sealing the record of the case.³⁶⁸

During the 83rd Regular Session, Texas leaders proposed legislation that would have expanded the collection, analysis, storage, use, and disclosure of DNA in Texas.³⁶⁹ Introduced by Representative Eiland, House Bill 1038 would have required every person arrested for a crime other than a class C misdemeanor³⁷⁰ to submit a sample of their DNA and pay a \$27 fee for its collection.³⁷¹ House Bill 1038 was considered in a formal meeting by the House Committee on Homeland Security and Public Safety on May 2, 2013, and reported favorably by a vote of 8-1 the next day.³⁷² The bill was then sent to the House Committee on Calendars, where it remained until session ended.³⁷³ House Bill 1063, introduced by Representative Luna, and Senate Bill 767, introduced by Senator Patrick, were companion bills that, like House Bill 1038, would have expanded the collection, analysis, and storage of DNA to persons convicted of class A misdemeanors or class B misdemeanors, as well as to person who were on deferred adjudications for public lewdness or indecent exposure.³⁷⁴ ³⁷⁵ Senate Bill 767 was reported favorably by the Senate Committee on Criminal Justice, but a motion to suspend the regular order of business to take up and consider it on May 3, 2013 was withdrawn after several senator express concerns with expanding mandatory DNA collection to misdemeanor convictions.³⁷⁶ House Bill 1063 was considered in a public hearing of the House Committee on Criminal Jurisprudence, but was left pending and never reported favorably.³⁷⁷

Seven days after the 83rd Regular Session ended, the United States Supreme Court ruled in *Maryland v. King* that a state law permitting the collection of DNA sample from a person arrested for certain serious crimes is constitutional and does not violate the Fourth Amendment.³⁷⁸ In 2009, Alonzo King was arrested for first-degree assault and was forced to

³⁶⁶ Tex. Gov't. Code § 411.153(a).

³⁶⁷ Tex. Gov't. Code § 411.153(b), (c), and (d).

³⁶⁸ H. Research Org., *Should Texas expand its DNA arrestee database?*, Tex. H.R. 83-8, Regular Sess., at 3 (2014).

³⁶⁹ H.B. 1038, 83rd Leg., Regular Sess. (Tex. 2013).

³⁷⁰ Class C misdemeanors are the lowest category of criminal offense and punishable by fine only.

³⁷¹ *Id.*

³⁷² *H.B. 1038 History*, Texas Legislative Information Service, <http://tllis/BillLookup/History.aspx?LegSess=83R&Bill=HB1038> (last visited Dec. 8, 2014).

³⁷³ *Id.*

³⁷⁴ S.B. 767, 83rd Leg., Regular Sess. (Tex. 2013).

³⁷⁵ H.B. 1063, 83rd Leg., Regular Sess. (Tex. 2013).

³⁷⁶ *S.B. 767 History*, Texas Legislative Information Service, <http://tllis/BillLookup/History.aspx?LegSess=83R&Bill=SB767> (last visited Dec. 8, 2014).

³⁷⁷ *H.B. 1063 History*, Texas Legislative Information Service, <http://tllis/BillLookup/History.aspx?LegSess=83R&Bill=HB1063> (last visited Dec. 8, 2014).

³⁷⁸ *Maryland v. King*, 133 U.S. 1958 (2013).

submit a sample of his DNA in accordance with the Maryland DNA Collection Act.³⁷⁹ That law requires the collection of a DNA sample from every person arrested for burglary, attempted burglary, or a violent crime, such as murder, rape, kidnapping, or first-degree assault, and the destruction of that sample if the charge does not result in a conviction.³⁸⁰ Thus, when Mr. King was arrested, law enforcement conducted a cheek swab during the booking process.³⁸¹ The DNA from the swab was then analyzed and matched to an unsolved rape case for which Mr. King was later convicted.³⁸² Seeking to overturn the conviction, Mr. King challenged the constitutionality of the cheek swab as an unreasonable search under the Fourth Amendment.³⁸³ In a 5-4 decision written by Justice Anthony Kennedy, the Supreme Court held that the custodial collection of DNA is constitutional when an arrest for a serious criminal offense is supported by probable cause.³⁸⁴

Justices Scalia, Ginsburg, Sotomayor, and Kagan dissented from the majority opinion in *King*.³⁸⁵ Writing for the minority, Justice Scalia argued that the Fourth Amendment categorically forbids suspicion-less searches, such as the search of Mr. King, and further noted that "taking DNA samples from arrestees has nothing to do with identifying them."³⁸⁶ Concluding his dissent, Scalia expressed his doubt that the writers of the Constitution intended for its provisions to be satisfied by a demonstration that a particular course of action is wise.³⁸⁷

*Today's judgment will...have the beneficial effect of solving more crimes; then again, so would the taking of DNA samples from anyone who flies on an airplane... applies for a driver's license, or attends a public school. Perhaps the construction of such a genetic panopticon is wise. But I doubt that the proud men who wrote the charter of our liberties would have been so eager to open their mouths for royal inspection. I therefore dissent, and hope today's incursion upon the Fourth Amendment...will someday be repudiated.*³⁸⁸

There has also been a debate in Texas over expanding the scope of DNA collection, analysis, storage, and use.³⁸⁹ The arguments of those engaged in that debate typically focus on privacy, public safety, and the availability of resources.³⁹⁰ Supporters argue expansion is the proper use of limited government resources, will improve public safety, and does not meaningfully violate privacy rights.³⁹¹ Opponents, on the other hand, argue expansion is a serious and unjustifiable violation of privacy that does not measurably improve public safety despite high costs, which only further strain limited state resources.³⁹²

³⁷⁹ *Maryland v. King*, 133 U.S. 1958 (2013).

³⁸⁰ *Id.*

³⁸¹ *Id.*

³⁸² *Id.*

³⁸³ *Id.*

³⁸⁴ *Id.*

³⁸⁵ *Maryland v. King*, 133 U.S. 1958 (2013) (Scalia, dissenting).

³⁸⁶ *Id.*

³⁸⁷ *Id.*

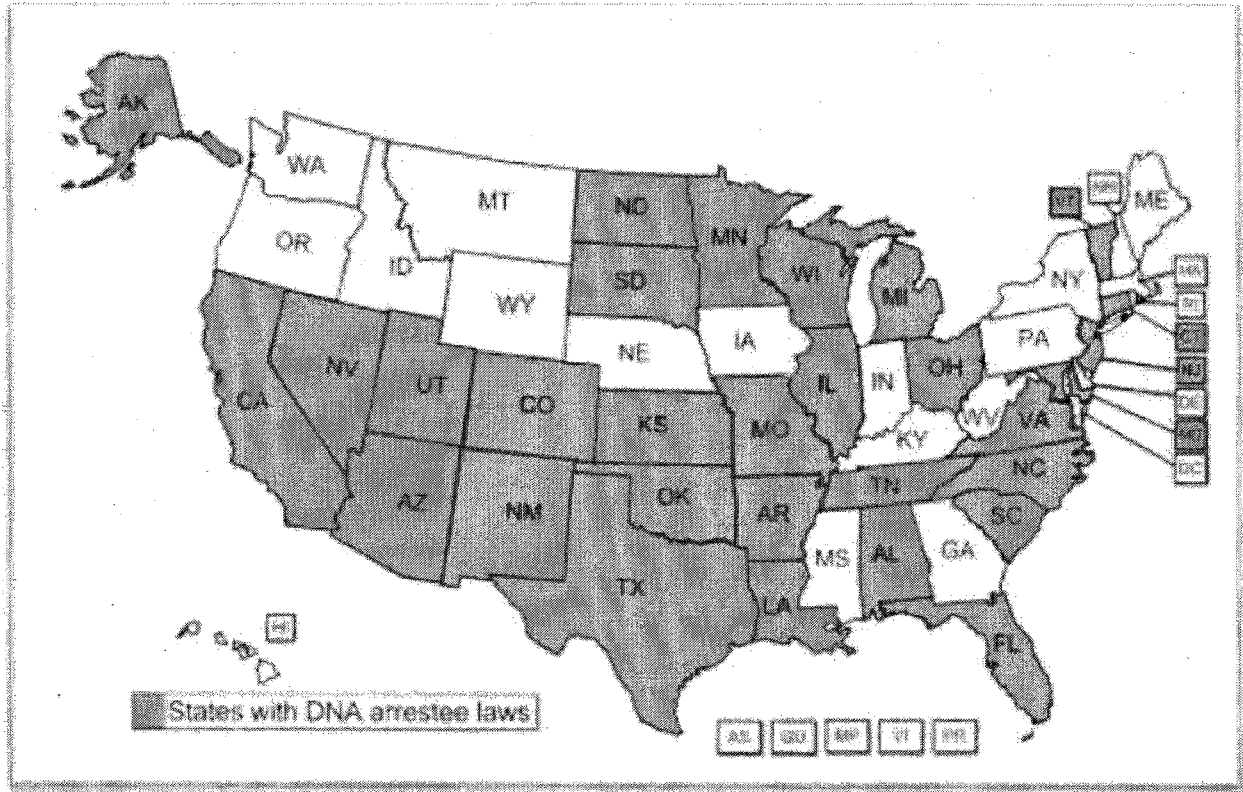
³⁸⁸ *Id.*

³⁸⁹ H. Research Org., *Should Texas expand its DNA arrestee database?*, Tex. H.R. 83-8, Regular Sess., at 6 (2014).

³⁹⁰ *Id.*

³⁹¹ *Id.*

³⁹² *Id.*



Source: National Conference of State Legislatures

Supporters say expanding the scope of DNA collection to those arrested or convicted of a class A or class B misdemeanor will improve public safety by providing law enforcement with additional information to investigate, solve, and prosecute crime.³⁹³ The National Institute of Justice explains it this way:

*CODIS can generate investigative leads in cases when a match is obtained. For example, if the DNA profile from a crime scene matches a sample taken from another crime scene, the cases may be linked in what is called a forensic hit. If the crime scene sample matches a convicted offender or arrestee sample, the result is called an offender hit. Hits give investigating officers valuable information that helps them focus their investigation.*³⁹⁴

According Department of Public Safety statistics, use of a DNA database aided 244 investigations in Texas this past August and has led to 2,336 offender hits for the year. In January 2013, the San Antonio Express-News reported that CODIS has helped Texas law enforcement solve more than 10,000 crimes and 643 homicides since 1996.³⁹⁵ Supporters also note that expansion would more quickly and accurately identify criminal suspects, which in some

³⁹³ H. Research Org., *Should Texas expand its DNA arrestee database?*, Tex. H.R. 83-8, Regular Sess., at 6 (2014).

³⁹⁴ *What is CODIS?*, National Institute of Justice, <http://www.nij.gov/journals/266/pages/backlogs-codis.aspx> (last visited Dec. 8, 2014),

³⁹⁵ Cindy Horswell, *DNA now spelling more guilty verdicts*, San Antonio Express News, Jan. 2, 2013, http://www.mysanantonio.com/news/local_news/article/DNA-now-spelling-more-guilty-verdicts-4159961.php

cases could exonerate a person wrongfully accused.³⁹⁶ Opponents of expansion do not contest that DNA information is useful, but claim the law already adequately protects public safety by requiring a DNA sample from convicted felons, persons charged with certain felonies, and arrestees with previous convictions.³⁹⁷ This, they say, ensures that a DNA sample is only taken from people who pose the greatest threat to the safety of the public.³⁹⁸ Furthermore, opponents state that a valid search warrant can be used to obtain a DNA sample, when Chapter 411 of the Government Code does not authorize its automatic collection.³⁹⁹ In the opponents' view, this limits collection to cases where there is probable cause, thus preventing the expansive and intrusive collection of DNA.⁴⁰⁰

In response to the opponents' argument that compulsory collection of DNA is a violation of privacy, supporters counter that DNA collection is a minimally invasive standard practice often used to confirm the identity of a criminal suspect.⁴⁰¹ They argue it is no different than a fingerprint or a mug shot, and note the Supreme Court reached a similar conclusion in *Maryland v. King*.⁴⁰² Supporters further assert that Texas law contains various safeguards for privacy, such as making the unlawful disclosure of a DNA record a state jail felony.⁴⁰³ Moreover, supporters argue that any valid privacy concerns are best solved by changing the law to allow automatic or expedited expunction for a non-conviction, not preventing expansion.⁴⁰⁴ Opponents, reply that DNA holds vastly more information than a fingerprint or a mug shot, and therefore is not similar to other standard booking procedures.⁴⁰⁵ They also point out that DNA is personal, intimate, and literally our blood, sweat and tears.⁴⁰⁶ Thus, they reason that DNA collection should not be required unless a person has been convicted of a serious crime.⁴⁰⁷ Finally, opponents assert that DNA databases are subject to abuse by law enforcement and unauthorized access by computer hackers.⁴⁰⁸ With Target and Home Depot as recent examples, opponents claim the tenuous nature of cyber security should not be ignored and the history of frequent database breaches not forgotten.⁴⁰⁹ A breach of a DNA database, they say, would have profound and far-reaching privacy implications.⁴¹⁰

Both sides also debate the issue of state resources. Supporters admit that state resources are limited, but argue greater compulsory DNA collection is justified to enhance public safety.⁴¹¹ Identifying dangerous criminals and repeat offenders, they say, is a critical function of

³⁹⁶ H. Research Org., *Should Texas expand its DNA arrestee database?*, Tex. H.R. 83-8, Regular Sess., at 6 (2014).

³⁹⁷ *Id.* at 7.

³⁹⁸ *Id.* at 7.

³⁹⁹ *Id.* at 7.

⁴⁰⁰ *Id.* at 7.

⁴⁰¹ *Id.* at 7.

⁴⁰² *Id.* at 7.

⁴⁰³ *Id.* at 7.

⁴⁰⁴ *Id.* at 7.

⁴⁰⁵ *Id.* at 8.

⁴⁰⁶ *Id.* at 8.

⁴⁰⁷ *Id.* at 8.

⁴⁰⁸ *Id.* at 8.

⁴⁰⁹ *Id.* at 8.

⁴¹⁰ *Id.* at 8.

⁴¹¹ *Id.* at 7.

government...⁴¹² Additionally, supporters note that if legislation like House Bill 1038 passes, the expenditure of state resources would be at least partially offset by imposing a fee on the person arrested, charged, or convicted for the collection of his or her DNA sample...⁴¹³ Opponents point out that, in February 2014, there were nearly 20,000 DNA samples that had not been tested in crime laboratories across the state...⁴¹⁴ They maintain that expanding the scope of DNA collection would only make that situation worse...⁴¹⁵ In so arguing, they point to the fiscal note for House Bill 1038, which estimates that expanding the scope of DNA collection could add as many as 460,000 samples to the current backlog, require an additional 80 full-time employees at DPS, and cost \$22.7 million biennially...⁴¹⁶ Opponents argue this is a substantial and unnecessary increase in the expenditure of resources that would be better utilized in other areas, such as transportation, education, or water...⁴¹⁷

Lastly, opponents argue that expanding the scope of DNA collection in Texas doesn't make sense given that the primary purpose of collecting and analyzing DNA is to assist law enforcement in the prevention and prosecution of crimes likely to involve DNA, such as murder and rape. These are crimes, opponents claim, where there is likely to be blood, hair, semen, or other types of biological evidence for which having a DNA sample is helpful either to confirm or alleviate suspicion. Yet, under House Bill 1038 and similar legislation, DNA would be collected from every person arrested for evading arrest on foot, burglary of a vending machine, claiming a fraudulent degree, promoting gambling, committing perjury, or any other misdemeanor...⁴¹⁸ These are crimes, according to opponents, where there is little likelihood DNA evidence would be helpful.

Mechanisms to ensure that private health care information is properly protected.

The protection of patient privacy and health care information has been an important part of the physician code of conduct since the creation of the Hippocratic Oath around the 4th Century B.C...⁴¹⁹ Since then, private health care information has increasingly been used by organizations and individuals who are not subject to medical ethics, such as pharmaceutical companies, health insurers, government program administrators, and attorneys. Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996 to address this, establishing rules certain health organizations must follow to ensure the protection of private health care information...⁴²⁰ Private health care information, also known as protected health information, is "individually identifiable health information" communicated or stored by a "covered entity"...⁴²¹ It typically includes information a doctor, nurse, or other health care provider entered in a

⁴¹² H. Research Org., *Should Texas expand its DNA arrestee database?*, Tex. H.R. 83-8, Regular Sess., at 8 (2014).

⁴¹³ *Id.* at 8.

⁴¹⁴ *Id.* at 7.

⁴¹⁵ *Id.* at 8.

⁴¹⁶ *Id.* at 8.

⁴¹⁷ *Id.* at 8.

⁴¹⁸ H.B. 1038, 83rd Leg., Regular Sess. (Tex. 2013).

⁴¹⁹ Peter Tyson, *The Hippocratic Oath Today*, PBS Online, March 27, 2001, <http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html>

⁴²⁰ H.R. 3103, 104th Cong. (1996) (enacted).

⁴²¹ *Summary of HIPPA Privacy Rule*, U.S. Department of Health and Human Services, <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html> (last visited Dec. 8, 2014).

medical record, information about a person in a health insurer's computer system, payment or billing information, and most other health information held by a covered entity.⁴²² Under HIPAA, covered entities, such as health plans,⁴²³ health care clearinghouses,⁴²⁴ and health care providers,⁴²⁵ must keep protected health information private and secure.⁴²⁶

To ensure the privacy of protected health information, the law determines to whom, for what purpose, and how much information may be used or disclosed.⁴²⁷ The general rule is that a covered entity may not use or disclose protected health information, except as permitted or required by the so-called Privacy Rule promulgated by the Department of Health and Human Services (HHS).⁴²⁸ Per that rule, a covered entity must disclose protected health information to the person who is the subject of the information, as well as the federal government to investigate or determine a covered entity's compliance with HIPAA.⁴²⁹ Although not required, disclosure is permitted when it is made (i) to a health care organization for essential health care functions, such as treatment, payment, and administrative operations; (ii) incident to a permitted or required use or disclosure; (iii) to clergy, friends, and family in certain situations, or (iv) for public policy purposes.⁴³⁰ Use or disclosure that is not permitted or required by the Privacy Rule must be authorized by the person who is the subject of the information.⁴³¹ The rule also requires that a covered entity make reasonable efforts to limit the use or disclosure of protected health information to only what is necessary to accomplish its purpose.⁴³² However, disclosures made to a health care provider for treatment, HHS, or the individual are exempted from this requirement.⁴³³ To assure compliance, the rule states that a covered entity must develop and implement procedures that limit access to health information and train employees on how to protect it.⁴³⁴

While the privacy of protected health information is important, policymakers are also concerned about its security, which is why the Security Rule and the Breach Notification Rule were promulgated.⁴³⁵ ⁴³⁶ Together, they ensure the security of electronic health information and hold

⁴²² *Summary of HIPAA Privacy Rule*, U.S. Department of Health and Human Services, <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html> (last visited Dec. 8, 2014).

⁴²³ Health plans include health insurance companies, HMOs, company health plans, and certain government programs that pay for healthcare, such as Medicare and Medicaid.

⁴²⁴ Healthcare clearinghouses process healthcare information and data.

⁴²⁵ Healthcare providers include most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.

⁴²⁶ *Summary of HIPAA Privacy Rule*, U.S. Department of Health and Human Services, <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html> (last visited Dec. 8, 2014).

⁴²⁷ *Id.*

⁴²⁸ *Id.*

⁴²⁹ *Id.*

⁴³⁰ *Id.*

⁴³¹ *Id.*

⁴³² *Id.*

⁴³³ *Id.*

⁴³⁴ *Id.*

⁴³⁵ *Summary of HIPAA Security Rule*, U.S. Department of Health and Human Services, <http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html> (last visited Dec. 10, 2014).

⁴³⁶ *Breach Notification Rule*, U.S. Department of Health and Human Services, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html> (last visited Dec. 10, 2014).

covered entities accountable for its care. Finally adopted on February 20, 2003, the Security Rule requires a covered entity to safeguard electronic protected health information from a "breach" with reasonable security measures, such as encrypting stored information; using passwords and personal identification numbers that allow only authorized individuals access to the information; and keeping a record of who accessed the information, when it was accessed, and what, if any, changes were made.⁴³⁷ In the event of a breach, however, the Breach Notification Rule requires that a covered entity, such as a doctor or a hospital, notify the Secretary of HHS and each person affected.⁴³⁸ The rule also forces a covered entity to notify prominent media outlets in the affected state or area if the breach affects more than 500 residents.⁴³⁹

Texas law incorporates much of HIPAA by reference and builds upon many of its mechanisms to protect private health care information.⁴⁴⁰ ⁴⁴¹ The statutory building process began in 2001 when Senate Bill 11 was passed, which added Chapter 181, Medical Records Privacy, to the Health and Safety Code.⁴⁴² The foundation laid by Senate Bill 11 includes defining "covered entity" more broadly than HIPAA,⁴⁴³ requiring patient consent for certain marketing activities,⁴⁴⁴ prohibiting the re-identification of de-identified data⁴⁴⁵ without the patient's consent,⁴⁴⁶ and authorizing an action by the attorney general for injunctive relief⁴⁴⁷ or a civil penalty.⁴⁴⁸ Atop the foundation laid by Senate Bill 11, the Legislature continued to build upon HIPAA by passing Senate Bill 1136 in 2003.⁴⁴⁹ That bill clarified the definition of "marketing",⁴⁵⁰ strengthened the requirement for patient consent to certain marketing activities, and added a provision allowing evidence of a covered entity's good faith effort to comply with the law to be considered by a court to "mitigate the imposition of an administrative penalty or assessment of a civil penalty."⁴⁵¹ Responding to amendments to HIPAA in 2009, House Bill 300 put the finishing touches on medical records privacy law in Texas.⁴⁵² That bill "strengthened penalties for wrongful disclosures, prohibited the sale of health data, set a floor for consent to share, and set standards for the training of health care professionals on privacy and security."⁴⁵³ House Bill 300

⁴³⁷ *Summary of HIPAA Security Rule*, U.S. Department of Health and Human Services, <http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html> (last visited Dec. 10, 2014).

⁴³⁸ *Breach Notification Rule*, U.S. Department of Health and Human Services, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html> (last visited Dec. 10, 2014).

⁴³⁹ *Id.*

⁴⁴⁰ Tex. Health & Safety Code § 181.001, 181.004, 181.005.

⁴⁴¹ This is done pursuant to an exception from preemption in HIPAA that expressly allows a state to provide greater privacy safeguards for individually identifiable health information.

⁴⁴² S.B. 11 77th Leg., Regular Sess. (Tex. 2001).

⁴⁴³ Tex. Health & Safety Code § 181.001(b)(2).

⁴⁴⁴ Tex. Health & Safety Code § 181.152(a).

⁴⁴⁵ Re-identification is a process by which individually identifying information is re-identified or connected to de-identified data (i.e. anonymous data) using the de-identified data and other data that is publically available.

⁴⁴⁶ Tex. Health & Safety Code § 181.151.

⁴⁴⁷ Tex. Health & Safety Code § 181.201(a).

⁴⁴⁸ Tex. Health & Safety Code § 181.201(b).

⁴⁴⁹ S.B. 1136 78th Leg., Regular Sess. (Tex. 2003).

⁴⁵⁰ Tex. Health & Safety Code § 181.001(b)(4).

⁴⁵¹ Tex. Health & Safety Code § 181.205(c).

⁴⁵² H.B. 300 81st Leg., Regular Sess. (Tex. 2009).

⁴⁵³ Senate Committee on State Affairs hearing, Sept. 16, 2014 (Testimony of Nora Belcher, Texas e-Health Alliance).

also "directed the Texas Health Services Authority to create a voluntary certification program, now known as SECURETexas," to certify covered entities for past compliance with state and federal medical records privacy and security law.⁴⁵⁴

Collectively, the bills discussed above created the Texas Medical Records Privacy Act (TMRPA). The TMRPA applies to covered entities under HIPAA and anyone else who comes into possession, obtains, or stores protected health information.⁴⁵⁵ However, it exempts covered entities that are regulated by another section of Texas law, such as life insurance companies, financial institutions, and employee benefit plans, and entities that interact only incidentally with protected health information, such as nonprofit agencies and crime victim compensation funds.^{456 457} A non-exempted covered entity must provide an employee with training on how to comply with state and federal law concerning protected health information.⁴⁵⁸ However, only the amount and type of training "necessary and appropriate" for a particular employee to perform his or her duties is required.⁴⁵⁹ In other words, the training can be tailored to a covered entity's line of business and to each employee's scope of employment.⁴⁶⁰ Thus, the training required for a janitor employed by a health insurance company can be much different than that required for a nurse working at a hospital. Whatever the training for an employee entails, it must be provided by a covered entity every two years.⁴⁶¹

An employee attending such a training would likely learn that several uses of protected health information are prohibited by law. For example, a person may not "reidentify or attempt to reidentify an individual who is the subject of any protected health information without obtaining the individual's consent..."⁴⁶² Texas is the only state in the nation with such a provision. The TMRPA also requires the "clear and unambiguous permission" to use or disclose protected health information for marketing purposes,⁴⁶³ unless the marketing is a face-to-face conversation,⁴⁶⁴ a promotional gift,⁴⁶⁵ necessary to administer a prescription drugs discount program,⁴⁶⁶ or the marketing is orally requested by the person receiving it.⁴⁶⁷ While these provisions are important, experts in this area of law view the prohibition on the sale of protected health information as the "crown jewel" of the TMRPA. Found in section 181.153 of the Health and Safety Code, the provision prevents a covered entity from disclosing "an individual's

⁴⁵⁴ Senate Committee on State Affairs hearing, Sept. 16, 2014 (Testimony of Nora Belcher, Texas e-Health Alliance).

⁴⁵⁵ *Id.*

⁴⁵⁶ Tex. Health & Safety Code, Chapter 181, Subchapter B.

⁴⁵⁷ Other examples include a workers' compensation fund or insurance company, the American Red Cross, mental health agencies, and educational records.

⁴⁵⁸ Tex. Health & Safety Code § 181.101(a).

⁴⁵⁹ *Id.*

⁴⁶⁰ Nora Belcher, *HB 300: Urban Legend Edition*, Presentation to Austin Bar Health Law Section (Jan. 22, 2013).

⁴⁶¹ *Id.*

⁴⁶² Tex. Health & Safety Code § 181.151.

⁴⁶³ Tex. Health & Safety Code § 181.152(a).

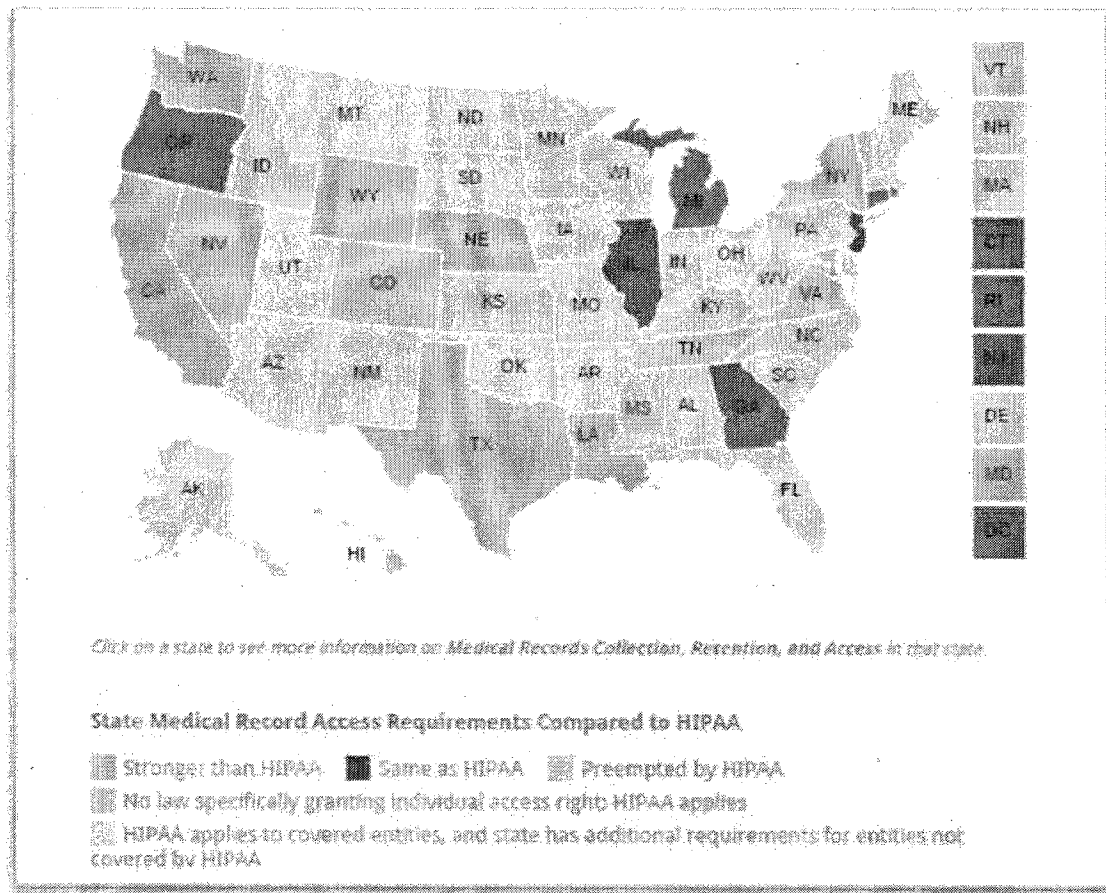
⁴⁶⁴ Tex. Health & Safety Code § 181.152(a)(1).

⁴⁶⁵ Tex. Health & Safety Code § 181.152(a)(2).

⁴⁶⁶ Tex. Health & Safety Code § 181.152(a)(3).

⁴⁶⁷ Tex. Health & Safety Code § 181.152(a)(4).

protected health information to any other person" for compensation,⁴⁶⁸ unless the disclosure is from a health care provider to a health insurance company for the purpose of treatment, payment, health care operations, performance of an insurance or health maintenance organization function,⁴⁶⁹ or is authorized or required by federal law.⁴⁷⁰



The map shows if a particular state's requirement is stronger than HIPAA (time a provider has to furnish the medical record once requested by the patient is shorter than HIPAA's 30-day period) or the same as HIPAA (meaning the state's law is a provider has 30 days from receipt of a patient's request to provide the medical records to the patient)
 Source: HealthInfoLaw.org

During a training required by the TMRPA, an employee might also learn that a person has a statutory right to access his or her medical records.⁴⁷¹ A hospital, for example, must make a patient's recorded health care information available to the patient no later than 15 business days after receiving written authorization.⁴⁷² Similarly, a doctor is required to provide a patient with a copy or summary of his or her medical record, billing record, or both within 15 business days following receipt of a written release for that information.⁴⁷³ Furthermore, any health care provider that uses an electronic health records system has a legal obligation to electronically

⁴⁶⁸ Tex. Health & Safety Code § 181.153(a).

⁴⁶⁹ Tex. Health & Safety Code § 181.153(a)(1).

⁴⁷⁰ Tex. Health & Safety Code § 181.153(a)(1).

⁴⁷¹ Tex. Occupations Code § 159.006(a).

⁴⁷² Tex. Health & Safety Code § 241.154(a).

⁴⁷³ Tex. Occupations Code § 159.006(d).

deliver a person's health record no less than 15 days after receiving a written request for it.⁴⁷⁴ According to George Washington University, the law for medical record access in Texas is stronger than HIPAA because federal law allows a longer thirty-day delivery period.⁴⁷⁵

For the violation of a prohibited act or any other provision of the TMRPA, the attorney general is authorized to institute an action for injunctive relief⁴⁷⁶ or civil penalties.⁴⁷⁷ The law limits the civil penalties that may be assessed to \$5,000 for each negligent violation,⁴⁷⁸ \$25,000 for each intentional violation,⁴⁷⁹ and \$250,000 for each violation in which a covered entity knowingly used protected health information for financial gain.⁴⁸⁰ The total amount of a penalty assessed against a covered entity is capped at \$250,000 per year, but only if the court finds the disclosure was made to another covered entity for treatment, payment, or health care operations, and that the information was either encrypted, the recipient of the information did not use or release it, or, at the time of disclosure, the covered entity had developed and implemented security and training policies to reduce the risk of disclosure.⁴⁸¹ However, if a court finds a pattern of violation it is authorized to assess a penalty of up to \$1.5 million annually.⁴⁸² Additionally, a covered entity licensed by an agency of this state, a doctor for example, is subject to "investigation and disciplinary proceedings, including probation or suspension," for a violation of the TMRPA.⁴⁸³ Furthermore, "if there is evidence that the violations are egregious and constitute a pattern or practice," the license of the covered entity may be revoked and the case referred to the attorney general.⁴⁸⁴ Lastly, a covered entity is "excluded from participating in any state-funded health care program if a court finds the covered entity engaged in a pattern or practice of violating" the TMPRA.⁴⁸⁵ To uncover violations, the TMPRA authorizes the Texas Health and Human Services Commission (HHSC) to request an audit by the Secretary of HHS or a licensing agency of this state.⁴⁸⁶

In addition to the TMPRA, Chapter 602 of the Insurance Code also establishes legal safeguards for the protection of private health information. There, the definition of a covered entity includes only insurance agents, health maintenance organizations, and insurance companies that are not "required to comply with the standards governing the privacy of individually identifiable health information" under HIPAA.⁴⁸⁷ ⁴⁸⁸ These covered entities must obtain permission from the

⁴⁷⁴ Tex. Health & Safety Code § 181.102(a).

⁴⁷⁵ George Washington University and the Robert Wood Johnson Foundation, *Individual Access to Medical Records: 50 State Comparison* (last visited on Dec. 10, 2014), <http://www.healthinfoworld.org/pdf/print/individual-access-medical-records-50-state-comparison>

⁴⁷⁶ Tex. Health & Safety Code § 181.201(a).

⁴⁷⁷ Tex. Health & Safety Code § 181.201(b).

⁴⁷⁸ Tex. Health & Safety Code § 181.201(b)(1).

⁴⁷⁹ Tex. Health & Safety Code § 181.201(b)(2).

⁴⁸⁰ Tex. Health & Safety Code § 181.201(b)(3).

⁴⁸¹ Tex. Health & Safety Code § 181.201(b-1).

⁴⁸² Tex. Health & Safety Code § 181.201(c).

⁴⁸³ Tex. Health & Safety Code § 181.202.

⁴⁸⁴ Tex. Health & Safety Code § 181.202(1)-(2).

⁴⁸⁵ Tex. Health & Safety Code § 181.203.

⁴⁸⁶ Tex. Health & Safety Code § 181.206(a)(1).

⁴⁸⁷ Tex. Ins. Code § 602.001, 602.002.

⁴⁸⁸ Section 602.002, Insurance Code states that "this chapter does not apply to a covered entity that is required to comply with the standards governing the privacy of individually identifiable health information adopted by the

person who is the subject of the information before disclosing nonpublic personal health information,⁴⁸⁹ which is any information about health status, provision of health care, or payment for health care that can identify an individual.⁴⁹⁰ However, a covered entity may disclose nonpublic health information "necessary to perform insurance or health maintenance organization functions,"⁴⁹¹ such as investigating fraud,⁴⁹² underwriting,⁴⁹³ risk management,⁴⁹⁴ or quality assurance.⁴⁹⁵ A covered entity under Chapter 602 of the Insurance Code is also required to comply with the provisions of Subchapter D, Chapter 181 of the Health and Safety Code and thus must not use protected health information for re-identification, marketing, or financial gain.⁴⁹⁶ The failure to comply with Chapter 602 can cost a person his or her business license, the eligibility to participate in state programs, and up to \$3,000 per violation, not to exceed \$250,000 annually.⁴⁹⁷

No matter where it is defined in Texas law, a covered entity must comply with the Identity Theft Enforcement and Protection Act and provide notification to a person affected by the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information."⁴⁹⁸ ⁴⁹⁹ The notification must be made to in-state and out-of-state residents as quickly as possible,⁵⁰⁰ but may be delayed at the request of a law enforcement agency that determines it will impede a criminal investigation or as is necessary to define the scope of the breach and restore the integrity of sensitive personal information.⁵⁰¹ In most instances, notice must be given in writing by mail, but in situations involving a breach affecting 500,000 or more people, notice can be given by e-mail, conspicuous website posts, or broadcast on major statewide media.⁵⁰² For out-of-state residents that live in a state with a similar law, notice under that law satisfies the Texas requirement.⁵⁰³ Failure to comply with the Texas Breach Notification Law may result in the assessment of a civil penalty not to exceed \$100 per affected person for each day a covered entity does not take "reasonable action" to provide notification, except that not more than \$250,000 may be assessed annually.⁵⁰⁴ As of

United States secretary of health and human services under Section 262(a), Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.).

⁴⁸⁹ Tex. Ins. Code § 602.051(a).

⁴⁹⁰ Tex. Ins. Code § 602.001(3).

⁴⁹¹ Tex. Ins. Code § 602.053.

⁴⁹² Tex. Ins. Code § 602.053(1).

⁴⁹³ Tex. Ins. Code § 602.053(2).

⁴⁹⁴ Tex. Ins. Code § 602.053(7).

⁴⁹⁵ Tex. Ins. Code § 602.053(10).

⁴⁹⁶ Tex. Ins. Code § 602.054(1).

⁴⁹⁷ Tex. Ins. Code, Chapter 602, Subchapter C.

⁴⁹⁸ Tex. Bus. & Com. Code § 521.053(a).

⁴⁹⁹ Sensitive personal information includes information regarding health status, the provision of healthcare, and the payment for healthcare services. According to one expert, the definition is "broad enough to include protected health information" as defined by HIPAA and TMRPA.

⁵⁰⁰ Tex. Bus. & Com. Code § 521.053(b).

⁵⁰¹ Tex. Bus. & Com. Code § 521.053(d).

⁵⁰² Tex. Bus. & Com. Code § 521.053(e), (f).

⁵⁰³ Tex. Bus. & Com. Code § 521.053(b-1).

⁵⁰⁴ Tex. Bus. & Com. Code § 521.151(a-1).

September 3, 2014, only four states – Alabama, New Mexico, and South Dakota – did not have a breach notification law.⁵⁰⁵

Ways to ensure that previously anonymous data is not improperly re-identified and marketed.

Anonymous data is information that has been de-identified or anonymized by a process called de-identification wherein individually identifying information, such as names or social security numbers, are erased, deleted, removed or redacted from a data set, which is typically nothing more than a spreadsheet containing a significant amount of information. The purpose of this process is to prevent data from being identified as belonging to a particular person. However, due to recent advances in computer science and engineering, the reverse process of re-identification has made de-identification less effective. Re-identification is a process by which individually identifying information is re-identified or connected to de-identified data using the de-identified data and other data that is publically available. For example, de-identified data in a data set that contains a person's birthday, gender, and zip code can be "easily identifiable" according to Harvard University's Data Privacy Lab and in some cases re-identified with nearly 100 percent confidence.⁵⁰⁶ Privacy expert and associate professor at the University of Colorado School of Law, Paul Ohm, explains the re-identification process this way:

You have one anonymized database, such as the Netflix database of movie ratings. The key is--if I know that someone is in the Netflix database and I know a little bit about the movies that that person likes and dislikes—maybe I read Joe's blog or I'm his Facebook friend or he was over at my house for dinner—I can identify him. It turns out I don't need to know much about his movie preferences. If I know three or four movies, I stand a good chance of re-identifying him. If it's six to eight, I have an excellent chance. This ability to re-identify is possible because there are other databases that provide missing information. So by putting together two databases I've actually learned more than either database can reveal by itself.⁵⁰⁷

In 1997, Massachusetts of Technology graduate student Latanya Sweeney "put two databases together" to re-identify the previously anonymous medical record of former Massachusetts governor William Weld "using only his date of birth, gender, and ZIP" from a "publicly available population register" (e.g., a voter list).⁵⁰⁸ Testifying before the Privacy and Integrity Advisory Committee of the Department of Homeland Security in 2005, Sweeney said that "87 percent of the population of the United State is uniquely identifiable by date of birth, gender, and their 5-

⁵⁰⁵ *Security Breach Notification Laws*, National Conference of State Legislatures, <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> (last visited Dec. 10, 2014).

⁵⁰⁶ Please visit www.aboutmyinfo.net to see how easily your de-identified data could be re-identified using only your birthday, gender, and zip code.

⁵⁰⁷ Melanie D.G. Kaplan, *Privacy: reidentification a growing risk*, www.SmartPlanet.com (last visited Dec. 10, 2014), <http://www.smartplanet.com/blog/pure-genius/privacy-reidentification-a-growing-risk/>

⁵⁰⁸ Department of Homeland Security Privacy and Integrity Advisory Committee hearing, June 15, 2005 (Testimony Latanya Sweeney, Carnegie Mellon University).

digit ZIP code."⁵⁰⁹ ⁵¹⁰ More recently, Ms. Sweeney this past year re-identified the previously anonymous data – in this case medical conditions and procedures, such as abortions, sexually transmitted diseases, and alcoholism – for 241 participants in the Personal Genome Project using those three key pieces of information: birth date, gender, and ZIP code.⁵¹¹ "By linking demographics to public records such as voter lists, and mining for names hidden in attached documents," Sweeney said, "we correctly identified 84 to 97 percent of the profiles for which we provided names."⁵¹²

While re-identification has been used by researchers with presumably good intentions, such as Ms. Sweeney, to demonstrate a powerful point, it has not been exclusively used for academic purposes. In 2006, Netflix released anonymous movie preference data gathered from the rankings of more than 500,000 customers over a six-year period.⁵¹³ The information was released as part of a \$1 million contest to improve Netflix's movie recommendation algorithm and was used to uniquely identify individual users.⁵¹⁴ For example, a person can identify ninety-nine percent of people in the Netflix database with as little information as six movie rankings and the date those rankings were made.⁵¹⁵ After awarding the \$1 million prize in 2009, Netflix announced plans for a second contest, again aimed at improving the algorithm used to predict what movies users will enjoy.⁵¹⁶ That contest, however, was cancelled after privacy experts called it "irresponsible" and expressed serious concerns that the data Netflix was planning to release was not truly anonymous or de-identified.⁵¹⁷ The New York Times reported that the data set for the second contest contained "more than 100 million entries" and included information about users' "ages, gender, ZIP codes, genre ratings and previously chosen movies."⁵¹⁸ Paul Ohm, then with Princeton University's Center for Information Technology Policy, said that if Netflix were planning on "revealing information tied to so few" he had no doubt that researchers, such as Ms. Sweeney, could re-identify it and predicted Netflix could face a lawsuit under the Video Privacy Protection Act (VPPA),⁵¹⁹ which generally bans the disclosure of personally identifiable records of "pre-recorded video cassette tapes or similar audio visual material."⁵²⁰ ⁵²¹

⁵⁰⁹ Department of Homeland Security Privacy and Integrity Advisory Committee hearing, June 15, 2005 (Testimony Latanya Sweeney, Carnegie Mellon University).

⁵¹⁰ Likewise, in *Simple Demographics Often Identify People Uniquely* Sweeney reported that fifty-three percent of people in the U.S. can be uniquely identified using his or her city or town of residence, gender, and date of birth.

⁵¹¹ Latanya Sweeney ET AL., "Identifying Participants in the Personal Genome Project by Name." *Data Privacy Lab*. April 24, 2013. Harvard University (last visited Dec. 10, 2014) < <http://dataprivacylab.org/projects/pgp/> >

⁵¹² *Id.*

⁵¹³ Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA Law Review 1701, 1720-22 (2010) (discussing Netflix competition to improve movie recommendation algorithm).

⁵¹⁴ *Id.*

⁵¹⁵ *Id.*

⁵¹⁶ Steve Lohr, *Netflix Awards \$1 Million Prize and Starts a New Contest*, N.Y. Times, (Sept. 21, 2009, 10:15 AM), <http://bits.blogs.nytimes.com/2009/09/21/netflix-awards-1-million-prize-and-starts-a-new-contest/>

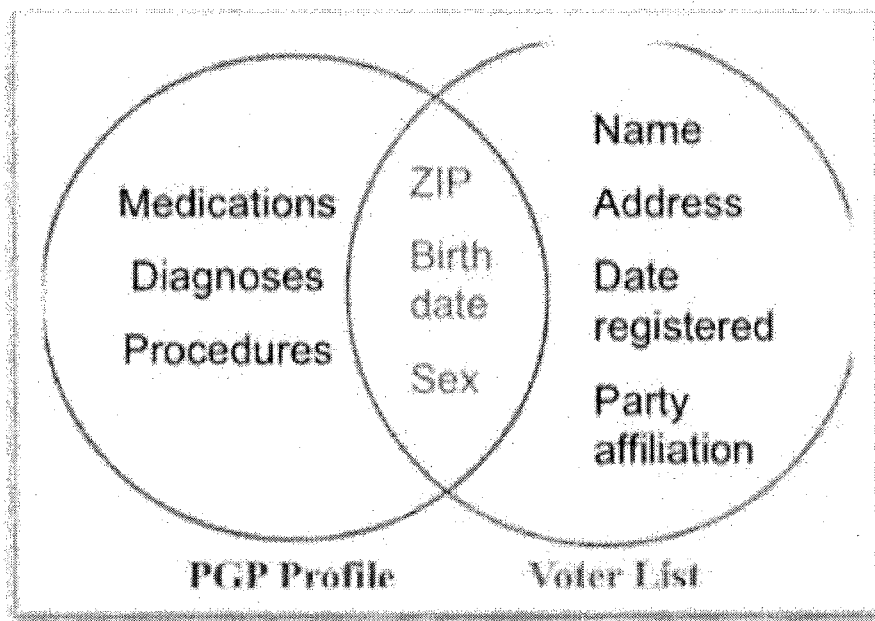
⁵¹⁷ David Coursey, *New "Irresponsible" Netflix Contest May Violate Customer Privacy*, PCWorld (Sept. 22, 2009, 9:57 AM), www.pcworld.com/article/172373/New_Irresponsible_Netflix_Contest_May_Violate_Customer_Privacy

⁵¹⁸ Steve Lohr, *Netflix Awards \$1 Million Prize and Starts a New Contest*, N.Y. Times, (Sept. 21, 2009, 10:15 AM), <http://bits.blogs.nytimes.com/2009/09/21/netflix-awards-1-million-prize-and-starts-a-new-contest/>

⁵¹⁹ David Coursey, *New "Irresponsible" Netflix Contest May Violate Customer Privacy*, PCWorld (Sept. 22, 2009, 9:57 AM), www.pcworld.com/article/172373/New_Irresponsible_Netflix_Contest_May_Violate_Customer_Privacy

⁵²⁰ 18 U.S. Code § 2710 (2014).

The improvement of movie recommendations is not the only commercial application of re-identification. For years, pharmaceutical manufacturers, or drug makers, have promoted their products through a process called "detailing."⁵²² When pharmacies, such as Walgreens or CVS, sell someone a drug, they receive prescriber information for that person.⁵²³ This information is de-identified and often sold to data miners who re-identify it to produce reports describing a particular person's drug-purchasing behavior.⁵²⁴ Those reports are leased to drug makers and used to "refine marketing tactics and increase sales to doctors."⁵²⁵ In recent years, this practice has come under increased scrutiny in state legislatures, such as Vermont. There, the state legislature in 2007 passed the Prescription Confidentiality Law, which generally prohibited prescriber information from being sold by a pharmacy, disclosed for marketing purposes, or used for marketing by a drug maker.⁵²⁶ Similar laws have also been passed in New Hampshire and Maine.⁵²⁸



A image of a Ven diagram that depicts how Ms. Sweeney used a voter list to match the names in a voter list to the medical conditions found in Personal Genome Project profiles. Source: Data Privacy Lab

A coalition of data miners and brand-name drug manufacturers brought suit in federal district court to challenge the Vermont law as a violation of their free speech rights under the First

⁵²¹ The Video Privacy Protection Act of 1988 was passed after a newspaper disclosed the video rental records of Supreme Court nominee Robert Bork.

⁵²² *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2656 (2011).

⁵²³ *Id.*

⁵²⁴ *Id.*

⁵²⁵ *Id.*

⁵²⁶ Vt. Stat. Ann. tit. 18, § 4631 (2007).

⁵²⁷ Despite the general rule, the law permitted prescriber information to be sold, disclosed, or used with the consent of the prescriber, for healthcare research or a criminal investigation, or if there was no reasonable belief the data could be re-identified.

⁵²⁸ Electronic Privacy Information Center, *IMS Health v. Sorrell*, https://epic.org/privacy/ims_sorrell/ (last visited Dec. 10, 2014).

Amendment to the United States Constitution.⁵²⁹ The state answered by arguing the law did not regulate speech, and even if it did, the law does not violate the First Amendment right to free speech because Vermont has a substantial interest in promoting public health, controlling health care costs, and protecting patient privacy.⁵³⁰ The District Court ruled for the state, but on appeal, the Second Circuit Court reversed, holding the law "unconstitutionally burdened the free speech of pharmaceutical marketers and data miners without adequate justification."⁵³¹ Having lost on appeal, Vermont petitioned the Supreme Court for review and on January 7, 2011, the Supreme Court granted certiorari.⁵³² In a 6-3 decision, the Court struck down Vermont's prescription privacy law.⁵³³ Writing for the majority, Justice Kennedy found that the Vermont law placed "content- and speaker-based restrictions on the sale, disclosure, and use" of prescriber information requiring application of the four-part Central Hudson test, which is a test to determine whether a law passes the intermediate level of scrutiny under which the Supreme Court examines a law abridging commercial speech.⁵³⁴ ⁵³⁵ Applying the Central Hudson test, the Court held that Vermont unconstitutionally "burdened a form of protected expression that it found too persuasive" while leaving "unburdened those speakers whose messages are in accord with its own views."⁵³⁶ According to the Court, "this the State cannot do."⁵³⁷ What a state could do, however, is enact a "more privacy-protective statute" that doesn't discriminate based on speaker or content. Explaining why such a law would likely withstand constitutional scrutiny, the Court writes:

The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure. In considering how to protect those interests, however, the State cannot engage in content-based discrimination to advance its own side of a debate. If Vermont's statute provided that prescriber-identifying information could not be sold or disclosed except in narrow circumstances then the State might have a stronger position. Here, however, the State gives possessors of the information broad discretion and wide latitude in disclosing the information, while at the same time restricting the information's use by some speakers and for some purposes, even while the State itself can use the information to counter the speech it seeks to suppress. Privacy is a concept too integral to the person and a right too essential to freedom to allow its manipulation to support just those ideas the government prefers.⁵³⁸

Despite growing concern for the privacy of personal data, the law in the United States does not provide for a general right to keep individual information private. While Congress has not passed

⁵²⁹ Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2656 (2011).

⁵³⁰ *Id.* at 2659.

⁵³¹ Sorrell v. IMS Health Inc., 631 F.Supp.2d 434 (D. Vt. 2009).

⁵³² *Proceedings and Orders*, Docket No. 10-779, United State Supreme Court (last visited Dec. 10, 2014), <http://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/10-779.htm>

⁵³³ Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2658 (2011).

⁵³⁴ *Id.* at 2663.

⁵³⁵ To pass the Central Hudson test a law must directly advance a substantial governmental interest in a way that is not more extensive than is necessary given that interest.

⁵³⁶ Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2672 (2011).

⁵³⁷ *Id.* at 2672.

⁵³⁸ *Id.* at 2671.

a comprehensive privacy law, there are federal statutes that protect certain categories of personal information. For example, the Fair Credit Reporting Act (FCRA) protects financial information under certain circumstances.⁵³⁹ and, as discussed above, HIPAA protects personal health information. Nevertheless, these laws typically do not protect information that has been de-identified. The Federal Trade Commission (FTC), for example, permits the use of de-identified financial information.⁵⁴⁰ Furthermore, regulations under the Gramm-Leach-Bliley Act (GLBA) exempt "blind data that does not contain personal identifiers such as account numbers, names, or addresses" from the law's privacy protections.⁵⁴¹ HIPAA regulations also allow the release of de-identified health information in some situations.⁵⁴² As demonstrated by Ms. Sweeney's research, however, the risk associated with not statutorily protecting de-identified data is that it is often re-identifiable using publically available information, such as birth date, gender, and ZIP code. The lack of federal protection against the possible re-identification of personal information has prompted state legislatures across the country to act, including Texas.

The action by Texas, however, has been limited. As with federal law, there is no general right to keep individual information private in Texas, nor is there a comprehensive privacy law that protects personal data from being re-identified and marketed. Texas law expressly protects only one narrow category of information from re-identification and marketing: protected health information. Under the TMRPA, it is generally unlawful to "re-identify or attempt to re-identify" another person using protected health information without his or her consent.⁵⁴³ In general, "clear and unambiguous" consent is also required to use protected health information for "any marketing communication."⁵⁴⁴ Relatedly, although not directly regulating the act of re-identification, section 34.008 of the Health and Safety Code defines de-identified data to include date of birth.⁵⁴⁵ This is a potentially significant development within the law given how easily data can be re-identified if a data set includes birthdates.

The re-identification prohibition under the TMRPA was passed in 2001 by Senate Bill 11,⁵⁴⁶ and Section 34.008 was added to the law in 2013 by Senate Bill 495.⁵⁴⁷ Outside of those bills, the only other piece of legislation related to the re-identification of personal data was Senate Bill 1620 from the 80th Regular Session of the Texas Legislature, which called for a study on the confidentiality of prescription information by the Texas State Board of Pharmacy.⁵⁴⁸ Senate Bill 1620 was considered in a public hearing of the Senate Committee on Health and Human Services on April 27, 2007, and reported favorably by a vote of 9-0 that same day.⁵⁴⁹ It later passed from

⁵³⁹ 15 U.S.C. § 1681 (2014).

⁵⁴⁰ Press Release, Federal Trade Commission, FTC Issues Final Commission Report on Protecting Consumer Privacy (March 26, 2012), <http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy>

⁵⁴¹ 12 C.F.R. 1022.20.

⁵⁴² 45 C.F.R. §164.502(d).

⁵⁴³ Tex. Health & Safety Code § 181.151.

⁵⁴⁴ Tex. Health & Safety Code § 181.152(a).

⁵⁴⁵ Tex. Health & Safety Code § 34.008(b)(1).

⁵⁴⁶ S.B. 11 77th Leg., Regular Sess. (Tex. 2001).

⁵⁴⁷ S.B. 495 83rd Leg., Regular Sess. (Tex. 2013).

⁵⁴⁸ S.B. 1620 80th Leg., Regular Sess. (Tex. 2007).

⁵⁴⁹ *S.B. 1620 History*, Texas Legislature Online,

<http://www.capitol.state.tx.us/BillLookup/History.aspx?LegSess=80R&Bill=SB1620> (last visited Dec. 10, 2014).

the Senate Floor without opposition and was referred to the House Committee on Public Health.⁵⁵⁰ Senate Bill 1620 was considered in a public hearing of that committee on May 16, 2007, but was left pending until session ended.⁵⁵¹

Recommendation

Texas law currently protects DNA samples and information by limiting who is required to submit a sample, the purposes for which the sample may be used, and the laboratories in which the samples can be processed. The Legislature should continue to monitor this issue to determine whether these protections are sufficient and work with stakeholders to decide if the expansion of compulsory DNA collection is necessary.

There are mechanisms in Texas law that protect the privacy of personal health care information. The re-identification, disclosure, sale, and use for marketing of protected health information is generally prohibited by Chapter 181 of the Health and Safety Code. These mechanisms are widely considered to be stronger than federal law and the law in many states. To ensure Texas continues to be a leader in protecting the privacy of personal health care information, the Legislature should continue to monitor the issue and observe the actions by other state legislatures.

Presently, Texas law ensures that previously anonymous data is not improperly re-identified and marketed in only one way: Section 181.151 of the Health and Safety Code bans it. The Legislature should continue to monitor the effectiveness of this ban to determine whether expanding it to other categories of personal information would be beneficial.

Charge No. 4

Examine possible reforms designed to increase citizens' ability to know what data is being collected about them by governmental and commercial entities and with whom that data is being shared, including an analysis of consumer informed consent. Examine related measures proposed or passed in other states.

"Informed consent" is an agreement to do something or to permit something to happen that is based on the disclosure of relevant facts necessary for the consenting party to make an intelligent decision, such as knowledge of the risks associated with the decision and alternative courses of action. The term is thought to have been first used by lawyer P.G. Gebhard in an amicus curiae brief on behalf of the American College of Surgeons for the case *Salgo v. Leland Stanford Jr. University* in 1957.⁵⁵² Conceptually, informed consent has three elements: disclosure, capacity, and voluntariness. These elements are satisfied when all the facts and information relevant to a particular decision are disclosed to a person with the capacity to make that decision who does so

⁵⁵⁰ *S.B. 1620 History*, Texas Legislature Online,

<http://www.capitol.state.tx.us/BillLookup/History.aspx?LegSess=80R&Bill=SB1620> (last visited Dec. 10, 2014).

⁵⁵¹ *Id.*

⁵⁵² Eric Pace, *P.G. Gebhard, 69, Developer of the Term 'Informed Consent'*, N.Y. Times, Aug. 26, 1997, <http://www.nytimes.com/1997/08/26/us/p-g-gebhard-69-developer-of-the-term-informed-consent.html>

voluntarily. Many believe that "informed consent is a fundamental protection for consumer privacy."⁵⁵³

Several federal laws require the informed consent of consumers for lawful disclosure of certain information. Enacted in 1988, the Video Privacy Protection Act (VPPA) generally prohibits the disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material," by a holder of those records, such as Blockbuster, unless the consumer who is the subject of the rental records consents in writing to its release.^{554 555 556} Several states have laws analogous to the VPPA, such as Michigan⁵⁵⁷ and Connecticut.⁵⁵⁸ Correspondingly, the federal government is generally prohibited by the Privacy Act of 1974 from disclosing "any record" without the prior written consent from "the individual to whom the record pertains" and must permit that individual to review, copy, or amend his or her records upon request.^{559 560} Lastly, the Children's Online Privacy Protection Act (COPPA), passed by Congress in 2000, requires a website operator to obtain parental consent prior to collecting personal information from a child under the age of thirteen and prohibits the conditioning of a child's participation in an online game with disclosure of "unnecessary" personal information.⁵⁶¹ Similar to the Privacy Act of 1974, COPPA also grants parents the right to review and delete any information collected by a website about their children.⁵⁶²

While few seem to oppose the protection of data privacy using informed consent, some skeptics criticize the mechanics of obtaining it in today's digital age.⁵⁶³ They claim that, under the law, obtaining consumer informed consent is often costly, cumbersome, slow, and in some cases, counterproductive.⁵⁶⁴ For example, regulations promulgated by the FTC under COPPA allow a parent to provide consent by mailing or faxing a paper form.⁵⁶⁵ Alternatively, parents may use their credit cards to provide consent under COPPA, but critics say this exposes parents to privacy risks as well. Given these issues, critics predict businesses may begin eliminating products or simply claiming that laws requiring consumer informed consent do not apply. Amazon, for

⁵⁵³ Mary DeRosa, *How Informed Consent Has Failed*, TechCrunch, July 26, 2014, <http://techcrunch.com/2014/07/26/how-informed-consent-has-failed/>

⁵⁵⁴ 18 U.S. Code § 2710 (2014).

⁵⁵⁵ Disclosure of personally identifiable movie rental information to law enforcement requires a warrant or court order. Evidence acquired in violation of the VPPA is excluded from criminal trials.

⁵⁵⁶ The VPPA has been called "one of the strongest protections of consumer privacy against a specific form of data collection."

⁵⁵⁷ Michigan Law § 445.1712.

⁵⁵⁸ Connecticut General Statute § 53-450.

⁵⁵⁹ 5 U.S.C. § 552a(b) (2014).

⁵⁶⁰ Exceptions to the Privacy Act's general rule against disclosure include (i) for statistical purposes by the Census Bureau and the Bureau of Labor Statistics, (ii) for routine uses within a U.S. government agency (iii) for archival purposes as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government (iv) for law enforcement purposes, (v) for congressional investigations, and (vi) other administrative purposes.

⁵⁶¹ 15 U.S.C. § 6502 (2014).

⁵⁶² 15 U.S.C. § 6502(b)(B) (2014).

⁵⁶³ Mary DeRosa, *How Informed Consent Has Failed*, TechCrunch, July 26, 2014, <http://techcrunch.com/2014/07/26/how-informed-consent-has-failed/>

⁵⁶⁴ *Id.*

⁵⁶⁵ 16 C.F.R. § 312.5(b)(i).

example, does not comply with COPPA because it claims it does not directly sell products to children.⁵⁶⁶ Other critics assert that informed consent has become ineffective, arguing it is caught in an analog age while the rest of the world has gone digital.⁵⁶⁷ Georgetown Law professor and former Deputy Counsel to President Obama, Mary DeRosa, writes that "the traditional mechanism for ensuring informed consent is hopelessly antiquated" and "long overdue for a wake-up call."⁵⁶⁸

*The underlying notion is that there are many uses of private information to which consumers will willingly agree, particularly if it means improved service or greater convenience. But each consumer is different, so they need sufficient information to make an informed decision. The traditional model for obtaining consent is to provide information in writing and seek agreement. With digital uses of data, this information usually comes in "terms of service" that are long and dense. Consumers rarely make their way through the information, and when they do they often find it complex and vague.*⁵⁶⁹

In February 2012, the Obama administration responded to these criticisms by releasing a "blueprint for privacy in the information age" titled *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy*. The report contains a Consumer Privacy Bill of Rights that sets forth "individual rights and corresponding obligations of companies in connection with personal data," such as individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.⁵⁷⁰ "Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones," wrote President Obama in introducing the Consumer Privacy Bill of Rights.⁵⁷¹ "One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever."⁵⁷²

In Texas, many state agencies have the legal authority to collect data on Texas residents and, in some instances, sell the information to private businesses without obtaining consent prior to its sale or providing an opportunity to opt-out. Perhaps the largest example is the Department of Motor Vehicles (DMV), which maintains a database with records for 22 million registered drivers and their vehicles.⁵⁷³ In 2012, the DMV generated \$2.1 million in revenue by selling information on Texas drivers from its database to more than 2,500 entities that ranged from

⁵⁶⁶ *Children's Online Privacy Protection Act*, Electronic Privacy Information Center (last visited Dec. 10, 2014), <https://epic.org/privacy/kids/>

⁵⁶⁷ Mary DeRosa, *How Informed Consent Has Failed*, TechCrunch, July 26, 2014, <http://techcrunch.com/2014/07/26/how-informed-consent-has-failed/>

⁵⁶⁸ *Id.*

⁵⁶⁹ *Id.*

⁵⁷⁰ The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy* (February 2012).

⁵⁷¹ *Id.*

⁵⁷² *Id.*

⁵⁷³ Mireya Villareal, *State Sells Personal Information & You Can't Opt Out*, CBS DFW, Feb. 11, 2013, <http://dfw.cbslocal.com/2013/02/11/cbs-11-investigates-your-personal-information-for-sale-you-cant-opt-out/>

collection agencies and banks to towing companies and private investigators.⁵⁷⁴ The Department of State Health Services (DSHS) also sells private data. According to one report, DSHS sold very sensitive data, such as prescriptions, medical tests, and diagnoses, collected from more than 27 million hospital visits to third parties over a twelve-year period from 1999 to 2010.⁵⁷⁵

As the above examples demonstrate, technological advances have made the collection and disclosure of personal data easier and more frequent, which is why privacy advocates assert that legal protections are needed to prevent abuses. A report by Attorney General Greg Abbott argues that Texas law should require a government agency to notify a person when his or her personal data is for sale and obtain his or her informed consent before selling it.⁵⁷⁶ Specifically, the report recommends reforming Texas law by adding a new chapter to the Government Code that regulates the sale of personal information to require a state agency get consent from the person who is the subject of the data before that data can be lawfully sold to a third party.⁵⁷⁷ While this would likely cause a slight decrease in state revenue, privacy advocates claim it would greatly increase the amount of control Texans can legally exercise over their personal information.

Another reform proposal to protect personal information is commonly called right-to-know legislation, which seeks to empower people to take responsibility for their personal data. Conceptually, the legislation accomplishes this by establishing a legal right for people to access their personal information and review with whom it has been shared. Right-to-know legislation has been proposed in California. There, Assembly Bill 1291, which is also known as the Right to Know Act, would require companies and state agencies to give people, upon request, access to the personal information those entities have digitally stored, as well as provide people a list of the third parties with whom the data has been shared.⁵⁷⁸ In addition to the possible reforms of informed consent and right-to-know, a third possibility is a prohibition of the resale of personal data by third parties and what is commonly called anonymous purchasing.⁵⁷⁹ This would stop the common practice of the repackaging and reselling of personal data by third parties to a fourth party, fifth party, and so-on. This reform provides a clear understanding of which parties can lawfully sell and possess personal data and which ones cannot.

Recommendation

Based on prior legislative measures both federally and in different states, there are several possible ways to reform Texas law to increase a citizen's ability to know what data is being

⁵⁷⁴ Mireya Villareal, *State Sells Personal Information & You Can't Opt Out*, CBS DFW, Feb. 11, 2013, <http://dfw.cbslocal.com/2013/02/11/cbs-11-investigates-your-personal-information-for-sale-you-cant-opt-out/>

⁵⁷⁵ Suzanne Batchelor, *Hospital patient privacy sacrificed as state agency sells or gives away data*, Austin Bulldog, Sept 30, 2010, www.reportingonhealth.org/fellowships/projects/hospital-patient-privacy-sacrificed-state-agency-sells-or-gives-away-data

⁵⁷⁶ Greg Abbott, *We the People Plan*, <http://abbotttownhall.wpengine.netdna-cdn.com/wp-content/uploads/2013/11/GregAbbottsWethePeoplePlanFINAL.pdf> (last visited Dec. 10, 2014).

⁵⁷⁷ *Id.*

⁵⁷⁸ A.B. 1291 2013-2014 Regular Sess. (Ca. 2013).

⁵⁷⁹ Anonymous purchasing is a technique used to enhance privacy by using disposable credit cards, bitcoins, or gift cards to limit, as much as possible, the personal information exchanged during a transaction.

collected about them by governmental and commercial entities. The Legislature should consider some or all of the following proposals:

- Make state agencies, before selling database information, acquire the consent of any individual whose data is to be released;
- Require companies and state agencies to give users access to the personal data the agency or company has stored on them – as well as a list of all the other companies with whom that original company or agency has shared the users' personal data – when a user requests it; and
- Prohibit data resale and anonymous purchasing by third parties.

Charge No. 5

Study the online legislative resources available to the public from Texas Senate Committee websites and compare resources to those provided by other state legislative committees in Texas and other states. Determine how Texas Senate websites can be improved to provide a more interactive and transparent government.

Interactive Forums

Lawmakers across the country are embracing the benefits of technology by gathering insight and ideas from constituents on a multitude of issues. Many of these lawmakers are using online discussion groups and conducting online opinion polls using various online tools. Recently, Lieutenant Governor Dewhurst implemented a similar interactive tool called *Your Texas Voice* where his office solicited public input on ideas for interim committee charges. Digital "town halls" and opinion polls will not completely replace public hearings, but with so many Americans using the internet to connect with political causes and issues online, these virtual venues are becoming increasingly popular.

Legislative websites throughout the U.S. have established new features to gather constituents' opinions about legislation during the session. Nevada posted an online opinion poll in 1999, which has been active every session since. Constituents can express opinions and vote on bills being considered.⁵⁸⁰ The website posts the comments, tallies the votes, and indicates which bills have received the most interest. These results are searchable by bill number, zip code, and Senate district. The New York Senate's Open Legislation website, created in 2009, allows visitors to view and comment on bills anonymously, as well as read comments from others.⁵⁸¹ Users can sign up to receive email updates that alert participants when comments are made on bills they are following. Several other states, including Alaska, Iowa, Wyoming, Maryland, North Dakota, and Washington, have also added online comment forums that allow constituents to state their views on specific bills.⁵⁸²

⁵⁸⁰ Pam Greenberg, *Virtual Venues: Legislators are reaping the benefits of reaching citizens online and paving the way for those who follow*, State Legislatures, July/August 2013.

⁵⁸¹ *Id.*

⁵⁸² *Id.*

In a study of a series of twenty online town hall meetings by members of Congress, the Congressional Management Foundation found virtual meetings increased participants' trust and their likelihood to vote.⁵⁸³ The study also discovered that the following elements contributed the most to the success of these online forums:

- Using a neutral moderator,
- Setting clear ground rules,
- Inviting a broad sample of participants,
- Allowing unscripted, real-time questions and comments from participants,
- Focusing on one timely issue, and
- Providing concise, unbiased information on the topic in advance.

However, the the time required for this kind preparation is often the biggest barrier to conducting online forms.⁵⁸⁴ A way around this may be to choose a very specific and salient subject at first and then to build on that.⁵⁸⁵

Other Initiatives: Recent Developments on the Texas Senate Website

In the world we live in today, people want access to information anytime and anywhere. Recently, the Texas Legislative Council, along with Senate Media and the Secretary of the Senate, undertook initiatives to address mobility issues and to engage members of the public in Senate policy making by updating the online Senate media player used to view hearings, and instituting an online witness registration pilot project for the summer and fall of 2014.⁵⁸⁶

Video streaming for Senate hearings has been available on the Senate website since 1999. Initially, the Senate used Real Player as its media player for Senate hearings. Although there were several issues with the quality and functioning of Real Player, by far its most troublesome aspect was its unavailability on mobile devices. The Texas Legislature recently upgraded the viewing system used to stream committee hearings from Real Player to a system called Granicus in late 2013. Granicus makes it much easier for the public to stream and view live and archived hearings. Not only does it address some of the previous quality and technical issues, but it also addresses the mobility issue. With Granicus, people can access live and archived hearings on their mobile devices whenever they want, wherever they want. Additionally, unlike Real Player, Granicus does not require a specific player agent in order to view live or archived video streams.

With the same goal of mobility in mind, the Senate is in the midst of an online witness registration pilot project, the Senate Witness Registration System, that began during the summer of 2014. The House of Representatives moved to an electronic witness registration system in the 83rd Legislative Session, which is explained in detail online.⁵⁸⁷ The House registration process is uniform for all House committees and the witness must be within reach of the Capitol's Wi-Fi

⁵⁸³ 21st Century Town Hall Meetings, Congressional Management Foundation, <http://www.congressfoundation.org/projects/town-hall/term/summary>

⁵⁸⁴ *Id.*

⁵⁸⁵ *Id.*

⁵⁸⁶ See Appendix to Charge 5.

⁵⁸⁷ To learn more please visit: <https://www.mytxlegis.legis.state.tx.us/hwrspublic/about.aspx>.

system to access the registration site. The Senate pilot witness registration program is similar to that of the House, with tweaks in the system to meet the different needs of the Senate.

Currently, anyone interested in testifying at a public hearing in the Senate is required to fill out a witness registration form by hand. The Senate Witness Registration System automates the witness registration process, the processing of witness testimony during a hearing, and the production of the witness list. The Senate Witness Registrations System is currently in a pilot phase with volunteer committees. If adopted, the use of the Senate Witness Registration System will be optional for each senate committee, as determined by the chair of the committee. Because use of the system would be optional, committees could determine on a hearing-by-hearing basis whether to use the system or hard copy witness cards to register witnesses. According to the Texas Legislative Council, all feedback on the pilot program from the participating committees has been positive.

Recommendation

The Committee recommends the Legislature continue to monitor and study ways to improve the online legislative resources available on the Texas Senate Committee websites.

Charge No. 6

Study the emerging negative impacts of the Federal Affordable Care Act, including the use of navigators, and make recommendations to mitigate any unintended consequences including rising health insurance premiums, lack of access to healthcare, mishandling of Texans' private information by insufficiently-trained navigators, and the Act's overall effect on Texas employers and insurance consumers. Evaluate free-market alternatives to the Act, including state-led proposals to repeal, reduce or replace the Act. Closely monitor and make recommendations on the continuation of the Texas Health Insurance Pool.

Background

The Patient Protection and Affordable Care Act, commonly called the Affordable Care Act (ACA), was adopted by Congress in March of 2010.⁵⁸⁸ The ACA, together with the Health Care and Education Reconciliation Act, represents the most significant regulatory overhauls of the U.S. healthcare system since Medicare and Medicaid were passed in 1965.⁵⁸⁹

The goals of the ACA are to increase the quality and affordability of health insurance by lowering the uninsured rate through the expansion of public and private insurance coverage and to reduce the costs of healthcare. It introduced several mechanisms in order to achieve these goals, including mandates, subsidies, and insurance exchanges.⁵⁹⁰ The ACA also requires

⁵⁸⁸ Patient Protection Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (Mar. 23, 2010), *as amended* by the Healthcare and Education Reconciliation Act, Pub. L. No. 111-152, 124 Stat. 1029 (Mar. 30, 2010).

⁵⁸⁹ Vicini, James; Stempel, Jonathan (June 28, 2012). "US top court upholds healthcare law in Obama Triumph" Reuters.

⁵⁹⁰ Pear, Robert (July 7, 2012). "Health Law Critics Prepare to Battle Over Insurance Exchange Subsidies". *New York Times*. Retrieved July 7, 2012 (http://www.nytimes.com/2012/07/08/us/critics-of-health-care-law-prepare-to-battle-over-insurance-exchange-subsidies.html?_r=0).

insurance companies to cover all applicants with minimum standards and to offer the same rates regardless of pre-existing conditions.⁵⁹¹

The United States Supreme Court considered several states' challenges to the ACA and issued its opinion on June 28, 2012, affirming in part and reversing in part the lower courts' opinions.⁵⁹² Although the Court ruled the individual mandate was not a valid exercise of Congress's power under the Commerce Clause, it upheld the provision under Congress's taxing power.⁵⁹³

The ACA requires states to provide access to an online marketplace, also called an exchange, where individuals and small businesses can purchase private insurance plans during the limited open enrollment period. States were given the option of establishing their own exchange, operating an exchange in cooperation with the federal government, or turning all administration of the health care marketplace over to the federal government.

Since the ACA was signed into law in 2010, Texas has reviewed and debated the different policy directives of the legislation. In a July 2012 letter sent to U.S. Health and Human Services Secretary Kathleen Sebelius, Governor Rick Perry announced that the state would not establish its own exchange.⁵⁹⁴ Instead, Texas opted to enter the federally run exchange. Although this decision took place prior to the Supreme Court's opinion on the constitutionality of the ACA, the Texas Legislature revisited Governor Perry's decision made during the 83rd Legislative Session and stayed in the federal exchange.

Texas is one of only six states that will not enforce the new health insurance reforms prescribed by the ACA. Under the Act, each state must enforce provisions and regulations related to the insurance exchange and market reforms unless it notifies the federal government that it cannot or will not. Texas, Arizona, Alabama, Missouri, Oklahoma, and Wyoming have all notified the federal government that they will not enforce the ACA. As a result, market reforms in Texas are regulated entirely by the federal government, and the Texas Department of Insurance (TDI) cannot enforce federal regulations. The federal Centers for Medicare and Medicaid Services will enforce the Act in all states that have refused to do so.

Texas Health Insurance Pool

The Texas Health Insurance Pool was created by the 79th Texas Legislature to provide health insurance to eligible Texas residents with preexisting medical conditions who were unable to obtain coverage from commercial insurers.⁵⁹⁵ As required by the federal Health Insurance Portability and Accountability Act of 1996, the Pool also served as the Texas alternative mechanism for individual health insurance coverage, guaranteeing portability of coverage to qualified individuals who lost coverage under a U.S. employer-based plan. The Pool began

⁵⁹¹The Henry J. Kaiser Foundation, *Obamacare and You: If You Have a Pre-Existing Condition* (Oct. 1, 2013) <http://kff.org/health-reform/fact-sheet/obamacare-and-you-if-you-have-a-pre-existing-condition/>

⁵⁹²Nat'l Fed'n of Indep. Bus. V. Sebelius, 132 S.Ct. 2566, 183 L.Ed.2d 450 (2012).

⁵⁹³*Id.*

⁵⁹⁴Letter from Governor Rick Perry to Secretary Kathleen Sebelius, U.S. Department of Health and Human Services (July 9, 2012) <http://governor.state.tx.us/files/press-office/O-SebeliusKathleen201207090024.pdf>.

⁵⁹⁵Acts 2005, 79th R.S., ch. 824, General and Special Laws of Texas.

issuing coverage in January 1998 to Texans who could not qualify for insurance due to pre-existing conditions and provided health benefits to more than 95,000 Texans..⁵⁹⁶

In response to the health insurance marketplace changes caused by the ACA, the 83rd Texas Legislature passed Senate Bill 1367, which abolished the Pool..⁵⁹⁷ Senate Bill 1367 authorized the commissioner of insurance to determine the date termination of the Pool's coverage and directed the Pool's board to develop a plan for dissolving the Pool. The Pool was originally set to dissolve on December 31, 2013, but the problematic rollout of the Healthcare.gov website caused the Texas Commissioner of Insurance to delay the cancellation of the Pool for 90 days, pushing back the cancellation date to March 31, 2014..⁵⁹⁸

During 2013, the Pool implemented a comprehensive campaign to educate policy holders about the new health insurance marketplace and ensure that all were fully aware that their Pool coverage would end March 31, 2014..⁵⁹⁹ The Pool developed a dissolution plan, which was approved by the commissioner of insurance. The pool has completed several phases of the dissolution plan, including termination on March 31, 2014 of all Pool insurance policies still in force. The Pool has informed the committee that all of its policy holders found alternative coverage before its termination.

Navigators

The ACA created the role of health insurance navigators to support and guide consumers through the process of finding appropriate health insurance. The United States Department of Health and Human Services is charged with establishing navigator standards and qualifications at the federal level. Navigators are funded by federal grants and can include community and consumer-focused nonprofit groups, unions, and professional associations. The ACA requires that each state have a navigator program by October 2013. Texas passed Senate Bill 1795 in the 83rd Legislative Session in order to preserve state control over the issue by giving TDI authority to regulate and establish a navigator program for the state..⁶⁰⁰

Senate Bill 1795 added a new chapter to the Insurance Code to regulate navigators for health benefit exchanges. It defined "navigator" as an individual or entity performing the duties described under 42 U.S.C. § 18031, including: (1) raise awareness of availability of health plans; (2) distribute information about enrollment in qualified health plans; (3) facilitate enrollment in qualified health plans; (4) offer services for enrollees with a grievance, complaint or questions regarding coverage; and (5) provide information that is culturally and linguistically appropriate for the population being served..⁶⁰¹

Senate Bill 1795 granted TDI the authority to oversee navigators in Texas and requires the commissioner to adopt rules necessary to meet the minimum requirements of federal law. The federal guidelines, which require navigators to "complete 20 to 30 hours of training, pass a

⁵⁹⁶ Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Katrina Daniel, Texas Dept. Insurance).

⁵⁹⁷ Acts 2013, 83rd R.S., ch. 615, General and Special Laws of Texas.

⁵⁹⁸ *Id.*

⁵⁹⁹ *Id.*

⁶⁰⁰ Acts 2013, 83rd R.S., ch. 1236, General and Special Laws of Texas.

⁶⁰¹ 42 USC §18031(i)(3).

certification test, and renew their certification annually," were released in July 2013.⁶⁰² On September 17, Governor Perry wrote a letter the Commissioner of TDI asking the organization to implement additional rules for navigators.⁶⁰³ Some of the additional rules requested were forty hours of additional training to supplement the federal standard, an additional training exam, and the ability for TDI to charge navigators for the services provided in overseeing their activities.

After two public hearings on the proposed rules and nearly 300 pages of written comments, TDI finalized rules to regulate navigators in Texas in response to feedback from stakeholders.⁶⁰⁴ These finalized rules took effect on February 10, 2014.⁶⁰⁵ The new rules require navigators to have completed state registration by March 1, 2014, and additional training by May 1, 2014.⁶⁰⁶ Among other changes, the new navigator rules reduced additional state training requirements from forty to twenty hours, prohibited navigators from offering advice on which plan is preferable, and added an exception for assisting a close relative.⁶⁰⁷ Many of the changes to the proposed rules are summarized in a one-page comparison from TDI, which can be found in the Appendix.⁶⁰⁸

The ACA Rollout in Texas

Under the ACA, individual and small employer group plans must cover a minimum package of essential health benefits beginning in 2014.⁶⁰⁹ The essential health benefits package is based on the coverage offered in the most popular plan in Texas' small group market, the BCBS BestChoice PPO.⁶¹⁰ Individual and small and large employer plans are required to provide certain preventive care services without cost sharing.⁶¹¹ Households with incomes between 100 and 400 percent of the federal poverty level may be eligible for premium and cost sharing subsidies.⁶¹²

Plans are offered in four categories of coverage levels, with the least expensive plan, the bronze tier, covering sixty percent of medical costs; plans in the silver tier cover seventy percent of costs; gold plans cover eighty percent; and the most expensive tier, platinum, covers ninety percent of medical costs.

Premium Increases

Many individuals who did not receive taxpayer subsidies to help pay for their premium are faced with higher deductibles, narrower networks, and higher premium. Premiums in the individual

⁶⁰² 45 CFR §155.215.

⁶⁰³ Letter from Governor Rick Perry to Insurance Commissioner Julia Rathgeber, Texas Department of Insurance (September 17, 2013).

⁶⁰⁴ Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Jamie Walker, Texas Dept. of Insurance).

⁶⁰⁵ *Id.*

⁶⁰⁶ *Id.*

⁶⁰⁷ *Id.*

⁶⁰⁸ See Appendix to Charge 6.

⁶⁰⁹ Texas Health Options, Texas Department of Insurance, <http://www.texashealthoptions.com/cp2/healthcare.html>.

⁶¹⁰ *Id.*

⁶¹¹ *Id.*

⁶¹² *Id.*

and small group market are increasing due to increased insurance product requirements and increased taxes and fees.⁶¹³

Starting on January 1, 2014, all health insurance policies were required to cover a broad range of mandated benefits, many of which were not previously included in policies. As a result, millions of people will be forced to purchase health insurance that is more comprehensive – and thus more expensive – than they previously had. This causes premiums to increase, because policies now must cover a substantially larger share of enrollees’ costs for health care (on average) and a wider range of benefits.

The ACA imposes a new sales tax on health insurance that increases the cost of health care coverage.⁶¹⁴ The amount of the tax will be \$8 billion in 2014, increasing to \$14.3 billion in 2018, and increasing based on premium trends thereafter.⁶¹⁵ The Joint Committee on Taxation estimates that the health insurance tax will exceed \$100 billion over the next ten years.⁶¹⁶ This tax will add a financial burden on families and small businesses in the form of increased premiums.

A new report from Milliman, Inc. helps explain how the ACA coverage expansion, new benefits, and market reforms will impact individual market health insurance premiums in 2014.⁶¹⁷ The report highlights how some provisions will increase premiums while others will make health care coverage more affordable for consumers.⁶¹⁸ The focus of this report is to highlight the broad range of changes happening in the marketplace and the wide variation in impact that is likely to occur. Highlights of the Milliman report include:

- Covering pre-existing conditions, requiring a broader benefits package, and covering uninsured Americans who have gone without medical care will benefit millions of people while increasing the cost of health care coverage. The new health insurance tax and other fees will also increase premiums.
- Other provisions of the law will make health care coverage more affordable, including premium and cost-sharing subsidies and the transitional reinsurance program, which provides funds to help offset the impact of high-cost enrollees.
- The impact on a specific individual will vary significantly depending on the individual's age, gender, location, health status, income level, and present coverage, if any. The report found that “young, healthy males could see substantial increases due to the combination of the overall rate change and the age/gender rating requirements” while “older, less healthy individuals could see rate reductions.”

⁶¹³ Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Annie Spilman, National Federation of Independent Business/Texas).

⁶¹⁴ America's Health Insurance Plans, *Health Insurance Tax*, <http://ahip.org/Issues/Premium-Tax.aspx>

⁶¹⁵ *Id.*

⁶¹⁶ *Id.*

⁶¹⁷ James T. O'Connor, *Comprehensive Assessment of ACA Factors That Will Affect Individual Market Premiums in 2014*, Milliman Report.

⁶¹⁸ *Id.*

- Individuals and families with household incomes up to 400 percent of the federal poverty level (FPL), or approximately \$94,200 for a family of four and \$45,960 for an individual, will be eligible for financial assistance to help lower total out-of-pocket insurance costs. The Milliman report estimates that those eligible for subsidies will receive financial assistance in 2014 to cover, on average, forty percent of the premium for the silver plan, and as much as ninety-four percent for those with the lowest incomes. Bronze plan premiums after subsidy could be as low as \$0 for certain low-income individuals.
- The report also notes that millions of people will not be eligible for subsidies and that the amount of the subsidy declines significantly as incomes rise. The Congressional Budget Office estimates that persons with incomes between 250-300 percent of the FPL will receive subsidies sufficient to cover forty-two percent of their premium and those with incomes between 350-400 percent will receive assistance to coverage thirteen percent of the premium.
- New benefit designs developed by health plans will lead to more affordable coverage options than would otherwise be available. These include wellness programs that encourage healthy living; prescription drug formularies that incentivize patients to choose lower-cost generic drugs when they are available; and the availability of “high-value networks” that are limited to providers with a track record of providing the high-quality care at the lowest cost.
- The report also highlights the importance of bringing younger and healthier people into the system to help make coverage as affordable as possible.

Texas Enrollment

Beginning January 1, 2014, most people were required to have qualifying health insurance coverage. In April 2014, the Obama administration announced that 8 million people signed up for coverage on the exchange during open enrollment.⁶¹⁹ The Department of Health and Human Services released exchange enrollment data in May for the entire six-month enrollment period.⁶²⁰

The first open enrollment period began October 1, 2013 and lasted through March 31, 2014. Early implementation efforts for the federal exchange received nearly universal disapproval. HealthCare.gov, the website where individuals apply for insurance through the federal exchange, crashed on opening and suffered from a myriad of problems throughout the first month. At the time, according to the United States Health and Human Services Department, 733,757 Texans signed up for medical insurance during the six-month open enrollment period that ended on March 31, 2014.⁶²¹ More Texans enrolled after March 1, 2014, than in the first five months of open enrollment. With 733,757 enrollees, Texas exceeded its target enrollment of 629,000 set by

⁶¹⁹ The White House, Office of the Press Secretary, (Apr. 17, 2014) <http://www.whitehouse.gov/the-press-office/2014/04/17/fact-sheet-affordable-care-act-numbers>.

⁶²⁰ The HHS data includes the additional supplemental enrollment period (SEP) reported through April 19, 2014.

⁶²¹ *Health Insurance Marketplace: Summary Enrollment Report for the Initial Annual Enrollment Period*, Department of Health and Human Services (May 1, 2014).

the Centers for Medicare and Medicaid Services in September 2013,⁶²² and has the third highest enrollment total in the nation behind California and Florida. However, it is important to note that this is only twenty-three percent of the estimated number of potential enrollees in Texas (733,757 out of more than 3.1 million).⁶²³

The closing of open enrollment means that those who have not signed up for a plan as of March 31, 2014 will face penalty fees when they file their 2014 federal tax returns. In 2014 adults without insurance will pay \$95 for the year, and \$47.50 per child younger than 18 years old, up to \$285 per family, or one percent of their annual household incomes, whichever is greater.⁶²⁴ In 2015, the penalties will increase to \$325 per year per adult, and \$162.50 per child, up to \$975 per family, or two percent of the annual household income, whichever is greater.⁶²⁵ Penalty fees are scheduled to increase each year that a person is not signed up for health insurance. There are exceptions for those with financial hardships, religious objections, qualifying Indian tribes, and others.⁶²⁶

A special enrollment period is generally granted for sixty days between now and Nov. 15, 2014, for people who have mitigating circumstances that affected their ability to gain health insurance, such as marriage, birth of a child, loss of health insurance, or other changes in family status. U.S. residents can sign up for health insurance or renew plans during the next open enrollment period, which is Nov. 15, 2014, through Feb. 15, 2015.

Number of Enrollees in the Texas Commercial Health Insurance Markets

Milliman was asked by the Texas Association of Health Plans to compile the results of a survey of its members. The survey solicited information on the number of enrollees in the Texas commercial health insurance markets (individual, small group, and large group) at various points in time since the end of calendar year 2013.⁶²⁷

Based on the survey responses, the individual market enrollment grew by ninety percent between December 31, 2013, and July 31, 2014, for an addition of 626,874 enrollees in this market.⁶²⁸ As of July 31, 2014, 45.5 percent (601,651) of the total individual enrollees were enrolled through the federal Marketplace, 14.4 percent (189,836) were enrolled in ACA-compliant plans outside of the Marketplace, and 40.1 percent (529,915) were enrolled in pre-ACA plans.⁶²⁹ A large increase in enrollment in the federal Marketplace came late in the open enrollment period, with

⁶²² *Projected Monthly Enrollment Targets for Health Insurance Marketplaces in 2014*, Centers for Medicare and Medicaid Services (Sept. 5, 2013).

⁶²³ John Davidson, *The Elusive Uninsured: Assessing the ACA Exchange in Texas*, Texas Public Policy Foundation (June 2014), available at http://www.texaspolicy.com/sites/default/files/documents/2014-05-PP20-ACAExchangesinTexas-CHCP-JohnDavidson_0.pdf

⁶²⁴ The Henry J. Kaiser Family Foundation, *The Requirement to Buy Coverage Under the Affordable Care Act* (2014), available at <http://kff.org/infographic/the-requirement-to-buy-coverage-under-the-affordable-care-act/>.

⁶²⁵ *Id.*

⁶²⁶ The Henry J. Kaiser Foundation, *A Guide to the Supreme Court's Affordable Care Act Decision* at 2 (July 2012) <http://www.kff.org/healthreform/upload/8332.pdf>.

⁶²⁷ Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Jamie Dudensing, Texas Association of Health Plans).

⁶²⁸ *Id.*

⁶²⁹ *Id.*

an eighty percent growth in Marketplace enrollment between the end of April and the end of July of 2014.⁶³⁰

Small group market enrollment decreased by seven percent, or a reduction of 71,891 members, from December 31, 2013 to July 31, 2014, for the responding entities.⁶³¹ As of July 31, 2014, 0.1 percent of enrollees were enrolled through the federal Marketplace, 22.2 percent were enrolled in ACA-compliant plans outside of the Marketplace, and 77.7 percent were enrolled in pre-ACA plans.⁶³²

The fully insured large group market enrollment stayed essentially the same during this same time period for the responding entities, with a total increase of 1,700 members (0.1 percent).⁶³³

Conflicting Federal Court Rulings on Subsidies

Conflicting Federal Court rulings raise questions about whether the ACA's subsidies should be available to consumers who purchase plans on the federal insurance exchange. The Internal Revenue Service (IRS) promulgated a rule that provides tax subsidies to low-income consumers who purchase health insurance on the federal exchange. This rule may conflict with the plain language of the ACA.

In *Halbig v. Burwell*, a panel of the U.S. Court of Appeals for the D.C. Circuit ruled in a two-to-one decision that subsidies to help people purchase coverage under the ACA should only be available in the exchanges set up by states, and not those run by the federal government.⁶³⁴ The court ruled that the statute narrowly, but explicitly, authorizes *only state-run exchange subsidies*, no matter what Congress may have intended.⁶³⁵ On the same day in a separate case, a panel of the U.S. Court of Appeals for the Fourth Circuit unanimously upheld the IRS's rulemaking in *King v. Burwell*.⁶³⁶ The Fourth Circuit found ambiguity in the text and said the IRS had the power to interpret the statute broadly as it set the rules.⁶³⁷ "Confronted with the Act's ambiguity, the IRS crafted a rule ensuring the credits' broad availability and furthering the goals of the law."⁶³⁸

On September 4, 2014, in response to a vote in favor by a majority of the judges eligible, the U.S. Court of Appeals for the D.C. Circuit granted the U.S. Secretary of Health's petition for rehearing the *Halbig* case en banc, vacating the earlier panel opinion.⁶³⁹ On November 7, 2014,

⁶³⁰ Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Jamie Dudensing, Texas Association of Health Plans).

⁶³¹ *Id.*

⁶³² *Id.*

⁶³³ *Id.*

⁶³⁴ *Halbig v. Burwell*, No. 14-5018, U.S. Court of Appeals for the District of Columbia Circuit (July 22, 2014).

⁶³⁵ *Id.*

⁶³⁶ *King v. Burwell*, No. 14-1158, U.S. Court of Appeals for the Fourth Circuit (July 22, 2014).

⁶³⁷ *Id.*

⁶³⁸ *Id.*

⁶³⁹ McGrail, Michael C. (Deputy Clerk of Court) (September 4, 2014). "Order (Granting Petition for Rehearing *En Banc*), *Halbig v. Burwell*, No. 14-5018". *U.S. Court of Appeals for the District of Columbia Circuit* (Amlaw.com). PACER Document 1510560.

the Supreme Court granted certiorari in the *King* case, with oral arguments expected to be held in March 2015 and a decision expected by late June or early July 2015.⁶⁴⁰

This split decision is notable because, if the Supreme Court decides to resolve the split, its decision could have a huge impact on Texas enrollees. Of the 733,757 Texans who selected a plan, eighty-four percent received financial assistance, including subsidies.⁶⁴¹ Accordingly, if it is determined that subsidies do not apply to federally-run exchanges, this large population of individuals, who otherwise would have qualified for federal subsidies, may not be able to afford insurance through the exchange, and thus, may be left without coverage and subject to penalties.

Effect On Texas Employers

Under the ACA, small business employers with fewer than fifty full-time workers, or full-time equivalent workers, will not be required to offer health insurance to their employees. However, the ACA encourages small business employers to provide health insurance by offering small business health care tax credits.⁶⁴² Many small businesses were already offering health insurance packages to their employees before the ACA was passed and signed into law. These plans are accepted or grandfathered in under the ACA.⁶⁴³

For small business owners who wish to change their coverage plans, or for those who did not offer health insurance before the new law, the ACA establishes the Small Business Health Options Program (SHOP).⁶⁴⁴ SHOP allows employers to compare and shop for insurance plans side by side for their employees. To be eligible for SHOP, small businesses must meet several requirements. In Texas, a business must have its primary business address located in the state. The other requirements concern employees.⁶⁴⁵ For a business to be eligible, it must have at least one common law employee and no more than fifty full-time equivalent (FTE) employees.⁶⁴⁶ The owner must offer health insurance coverage received through SHOP to all employees.⁶⁴⁷

Employers with fifty or more full-time and FTE employees may be required to pay tax assessments if their employees receive subsidized coverage through the marketplace because the employer does not offer minimum coverage or because the coverage offered is unaffordable.⁶⁴⁸ However, the IRS has delayed the penalty until 2015.⁶⁴⁹ Therefore, employers will not be penalized in 2014 for not offering affordable coverage of minimum value.⁶⁵⁰ Nevertheless, this delay creates uncertainty among businesses and is frustrating to some business owners.

⁶⁴⁰ Denniston, Lyle (November 7, 2014). "Court to rule on healthcare subsidies". *SCOTUSblog*.

⁶⁴¹ Senate Committee on State Affairs Hearing, Sept. 15, 2012 (testimony of Stacey Pogue, Center for Public Policies and Priorities).

⁶⁴² Texas Health Options, Texas Department of Insurance, <http://www.texashealthoptions.com/cp2/healthcare.html>.

⁶⁴³ *Id.*

⁶⁴⁴ Small Business's Introduction to the Affordable Care Act Part 1, NFIB Research Foundation, available at <http://www.nfib.com/Portals/0/PDF/AllUsers/research/studies/ppaca/nfib-aca-study-2013.pdf>.

⁶⁴⁵ *Id.*

⁶⁴⁶ *Id.*

⁶⁴⁷ *Id.*

⁶⁴⁸ Texas Health Options, Texas Department of Insurance, <http://www.texashealthoptions.com/cp2/healthcare.html>.

⁶⁴⁹ Small Business's Introduction to the Affordable Care Act Part 1, NFIB Research Foundation, available at <http://www.nfib.com/Portals/0/PDF/AllUsers/research/studies/ppaca/nfib-aca-study-2013.pdf>.

⁶⁵⁰ *Id.*

The National Federation of Independent Business (NFIB) conducted a study to examine the ACA's impact on Texas Employers and found that there are four main components: cost, economic impact, administrative burdens, and uncertainty.⁶⁵¹

According to NFIB's testimony at the Senate Committee on State Affairs hearing on September 15, 2014, the rising cost of health insurance is the biggest problem for small businesses.⁶⁵² NFIB found that sixty-four percent of small-business owners experienced a premium increase between 2012 and 2013.⁶⁵³ According to IRS data, between 2010 and 2013 (information for 2014 will be available later this year), average family premiums for small businesses have increased by \$1,341 (11.2%) in Texas.⁶⁵⁴

An NFIB study also found that the new mandates and taxes are having a negative economic impact on Texas businesses. Increased employee health benefit costs mean less investment in business and less hiring. The health insurance tax (HIT) on individual and small group policies will increase premiums by \$145 billion over the next decade.⁶⁵⁵ According to the study, Texas will lose at least 7,750 jobs and at least \$1.34 billion in economic activity as a result of the HIT tax by 2022.⁶⁵⁶

Additionally, the ACA imposes new administrative burdens on small and large businesses. Nearly all small businesses must provide their employees with a "Notice of Coverage Options" document that describes the federal exchange and employer-sponsored insurance, if it is provided.⁶⁵⁷ Offering small businesses must also provide a "Summary of Benefits and Coverage" document that describes the employer-sponsored insurance in plain language. Applying for health insurance is more cumbersome for individuals and small businesses as the federal government requires more information than was previously required. Small businesses provide this information to their insurance company, which then provides it to the federal government.

Large businesses also face administrative burdens. Calculations for the employer mandate will have to be made this year and next year, so employers must keep close track of employees' hours.⁶⁵⁸ The IRS regulations that determine whether a business is subject to the employer mandate are complex and spans 227 pages.⁶⁵⁹ Reconciling and reporting this employer mandate

⁶⁵¹ See Appendix to Charge 6 (NFIB written testimony).

⁶⁵² *Id.*

⁶⁵³ Small Business's Introduction to the Affordable Care Act Part 1, NFIB Research Foundation, *available at* <http://www.nfib.com/Portals/0/PDF/AllUsers/research/studies/ppaca/nfib-aca-study-2013.pdf>.

⁶⁵⁴ Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Annie Spilman, National Federation of Independent Businesses Texas).

⁶⁵⁵ Small Business's Introduction to the Affordable Care Act Part 1, NFIB Research Foundation, *available at* <http://www.nfib.com/Portals/0/PDF/AllUsers/research/studies/ppaca/nfib-aca-study-2013.pdf>.

⁶⁵⁶ *Id.*

⁶⁵⁷ Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Annie Spilman, National Federation of Independent Business/Texas).

⁶⁵⁸ *Id.*

⁶⁵⁹ *Id.*

information to the IRS are also complicated. These final regulations were an additional 84 pages.⁶⁶⁰

According to NFIB, the most frustrating component of the ACA to small business owners is the uncertainty surrounding the law. Several events have altered the ACA's implementation since its enactment in 2010. Most notably, the Obama administration unilaterally delayed the implementation of the employer penalty and part of the small business health exchanges from 2014 to 2015. These delays have added to the uncertainty over the potential effects of the ACA on small businesses. Texas is allowing small-business owners to keep their current policies for an additional year, delaying the cost increases associated with full compliance.⁶⁶¹ Regardless, many small-business owners are unable to predict the cost of renewal once their plans must come into full compliance.

Provider Challenges

The ACA brings challenging administrative changes to Texas Providers. The combination of administrative challenges and a general lack of health care literacy about insurance coverage has resulted in a very confused health care marketplace for both health care providers and the newly insured.

Impact of Narrow Networks on Access To Care and Greater Out-of-Pocket Costs

Narrow network plans have become increasingly popular in recent years, growing from fifteen percent of the insurance plans that employers offered in 2007 to twenty-three percent in 2012.⁶⁶² These narrow networks have been utilized more lately for products sold in the exchange.⁶⁶³ Accordingly, although narrow networks are not a new concept, their impact is exacerbated as a result of the ACA. Health plans often advertise that they have certain physicians, hospitals, and health care providers contracted to provide services, making it appear they have very robust networks from which a patient may access health care.⁶⁶⁴ This can be misleading to consumers when the provider network advertised is not always applicable for certain products or services. Patients who purchase coverage with a low premium rate may find out later about the limited or narrow network they are required to use and end up paying higher out-of-pocket costs if they fail to use the narrow network. The use of narrow networks and the confusion around them is often compounded when physicians are misrepresented as part of the network when they are not, and vice versa. Below are preliminary results from Texas Medical Association's 2014 Annual Survey demonstrating the frequency of provider directory misrepresentation.

Coverage Differentiation Needed -- Patient Identification Cards/Electronic Eligibility Verifications

⁶⁶⁰ *Id.*

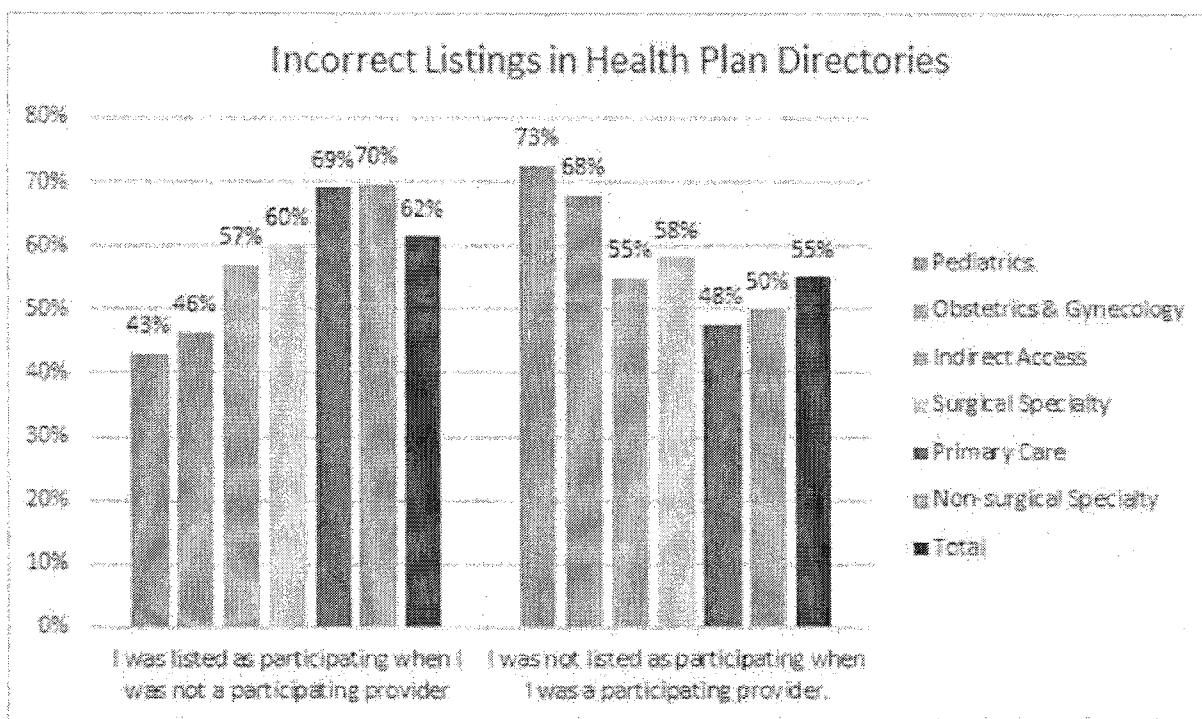
⁶⁶¹ State Responses to Administration Policy on Coverage Extensions, America's Health Insurance Plans, <http://www.ahipcoverage.com/2013/11/20/map-of-the-day-state-decisions-on-administrations-policy-on-coverage-extensions/>.

⁶⁶² Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Patrick Carter, M.D., Texas Medical Association).

⁶⁶³ *Id.*

⁶⁶⁴ *Id.*

Many insurers are offering products both inside and outside the exchange. Those products can encompass commercial Health Maintenance Organizations (HMOs) and Preferred Provider Organizations (PPOs) outside the exchange and qualified HMO and PPO plans inside the exchange that were purchased with and without premium subsidies. According to the Texas Medical Association, a physician's office needs to be able to determine from the patient's identification card or from standard electronic eligibility verifications whether the coverage is a private commercial plan, a qualified health plan (QHP), or a QHP that is subsidized.⁶⁶⁵ It will be imperative for a physician's office to be able to discern what type of coverage each patient has, as well as whether or not the coverage was paid in part with a premium subsidy and subject to the ninety-day grace period discussed further below.



Impact of the ACA's 90 Day Grace Period

Under the ACA, persons who receive a subsidy also have the benefit of a ninety-day grace period to bring premium payments current when they are in arrears. The ninety-day grace period's impact on services provided to patients with subsidized premiums makes it important to know whether a patient has a subsidized or non-subsidized premium.⁶⁶⁶ The federal government requires insurance companies to cover services for the first thirty days of the grace period. For the remaining sixty days of the grace period insurance companies are permitted to retroactively terminate the insurance policy should premium payments not be made by the covered person at the end of the 90 days. This means that insurance companies may demand that payments made to physicians be returned. Physicians then must attempt to collect directly from the patient for services they may have performed months before. Collection efforts are costly, disruptive, and

⁶⁶⁵ Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Patrick Carter, M.D., Texas Medical Association).

⁶⁶⁶ *Id.*

not always successful. The effect of the grace period may be cost increases on those who do pay for the services they receive..⁶⁶⁷

Free Market Alternatives: Self-Insurance

According to the Texas Public Policy Foundation, one possible state-based alternative to the ACA's individual mandate is to create a self-insurance program whereby individuals could be issued a certificate of authority by TDI if they set aside a certain percentage of monthly income to pay for medical expenses..⁶⁶⁸

By taking this savings-based approach, individuals could fulfill the ACA's individual mandate without having to purchase costly coverage through the exchange or, for those who work at small firms, rely on employers to provide insurance..⁶⁶⁹ An individual with a certificate of authority from TDI would be able to insure a spouse and dependents as a dedicated self-insurer, in compliance with the ACA's individual mandate..⁶⁷⁰

A version of this proposal was passed by the Texas House last session. House Bill 2732 created a self-insurance program but set very high capital requirements. An amended draft version of the bill swaps capital requirements for a percentage of monthly income, capped at a certain amount..⁶⁷¹

Such a program could be further modified by being coupled with a state-sponsored reinsurance program for self-insured individuals, which would protect self-insurers from severe losses at the outset and prompt more Texans to choose self-insurance over costly ACA exchange coverage, or no coverage at all..⁶⁷²

Recommendation

This report has sought to provide a detailed description of the rollout of the ACA in Texas. However, because of the timing of this report, there are still far more questions than answers regarding the success or failure of the ACA's implementation in Texas. The Committee recommends that the Legislature continue to monitor the ACA's implementation in Texas and address the following questions during the 84th Legislative session:

- What will happen to competition and premiums in the Texas marketplace in 2015 and beyond?
- To what degree was the transfer of data between the marketplace and health insurance successful? How many people who thought they purchased insurance actually fell through the cracks of a flawed rollout?

⁶⁶⁷ Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Patrick Carter, M.D., Texas Medical Association).

⁶⁶⁸ Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of John Davidson, Texas Public Policy Foundation).

⁶⁶⁹ *Id.*

⁶⁷⁰ *Id.*

⁶⁷¹ *Id.*

⁶⁷² *Id.*

- Are the newly-insured using the healthcare system appropriately?
- Did people make well-informed decisions about which tier and specific insurance product to buy?

Finally, the Legislature should continue to monitor how the ACA affects the number of uninsured in the state, the ability of patients to access providers, and costs to the state healthcare system.

Charge No. 7

Study and make recommendations on increasing medical price transparency in Texas, including studying the impact of Senate Bill 1731, 80th Legislative Session. Analyze relevant reforms considered or implemented in other states, and make recommendations regarding potential changes designed to create a more open marketplace for enhanced consumer decision making in Texas.

Medical Price Transparency

In recent years, the rising cost of health care has been a prevalent point of discussion and debate for employers, providers, health plans, and patients. A major part of this discussion is the potential for inaccurate information and the absence of transparency in the costs of health care services. Disclosure of this information may help patients make appropriate and cost-effective health care choices.

However, the healthcare marketplace is complex. Prices vary by payer, and government programs like Medicare and Medicaid set rates, which may be below the cost of providing care.⁶⁷³ Providers typically have contractually negotiated rates with numerous health plans. As a result, the lack of price information is becoming a significant issue for both insured and uninsured patients. Internet sites, such as FairHealth and Health Care Bluebook, provide patients with charge information that is characterized as "a fair price to pay for a service or product" when paying cash at the time of treatment.⁶⁷⁴ Additionally, many insurers offer charge as well as payment information for their insureds via a "cost estimator" program on the insurers' websites. Even with this movement towards transparency, patients may still find it difficult to determine medical price information in certain circumstances.

To be effective, price transparency must offer clear information that is readily accessible to patients and enables them to make meaningful comparisons among providers. It also requires a collaborative effort among providers, care purchasers, and payers to identify and develop the information and tools that will be most useful to patients.⁶⁷⁵ According to the Healthcare Financial Management Association (HFMA), price transparency should ultimately provide

⁶⁷³ Senate Committee on State Affairs hearing, Sept. 15, 2014 (Testimony of Patrick Carter, M.D., Texas Medical Association).

⁶⁷⁴ *Id.*

⁶⁷⁵ Price Transparency in Healthcare, Report from the HFMA Price Transparency Task Force, Healthcare Financial Management Association (2014).

patients with the information they need to understand the total price of their care and what is included in that price.⁶⁷⁶

Healthcare Literacy

Health insurance companies are concerned by the lack of health care literacy among consumers and the impact it is having on price transparency efforts. Under the Affordable Care Act (ACA), newly-insured patients are gaining coverage, which results in increased exposure to healthcare costs. Consumers have an urgent need for meaningful and transparent price information. Patients are being asked to act as consumers in a marketplace in which price, a fundamental driver of consumer behavior, is often unknown until after the services they purchase have been performed.⁶⁷⁷

Texans need to become better educated on health care costs and services so they are able to make better choices, regardless of whether they have coverage. According to the National Assessment of Adult Literacy, only twelve percent of all Americans have a proficient level of health literacy to make decisions.⁶⁷⁸ For the health care system in Texas to function at maximum efficiency, consumers and patients need a better understanding of their health care in general. Without this information, consumers are prevented from engaging in comparative shopping based on price, quality, and family needs.

Education of the public on health care spending cannot be ignored.⁶⁷⁹ As the increase in financial responsibility shifts toward consumers on both in and out-of-network services, they need to be involved in their health spending decision-making, but need more education to do this wisely. Education of the public on their health care spending, and how to best budget such spending, is imperative to the long term stability of the healthcare market.⁶⁸⁰

Transparency Framework

Because health plans will, in most instances have the most accurate data on prices for their members, they should serve as the principal source of information for their members.⁶⁸¹ As noted earlier, many health plans already have a Internet-based tool available for their members. These tools have the potential to benefit both patients and health plans, providing patients with needed information while strengthening the health plan's value to its members.⁶⁸²

⁶⁷⁶ Price Transparency in Healthcare, Report from the HFMA Price Transparency Task Force, Healthcare Financial Management Association (2014).

⁶⁷⁷ Price Transparency in Healthcare, Report from the HFMA Price Transparency Task Force, Healthcare Financial Management Association (2014).

⁶⁷⁸ National Network of Libraries of Medicine; health literacy, <http://nnlm.gov/outreach./consumer/hlthlit.html>.

⁶⁷⁹ Senate Committee on State Affairs hearing, Sept. 15, 2014 (Testimony of Carl Isett, Texas Association of Benefit Administrators).

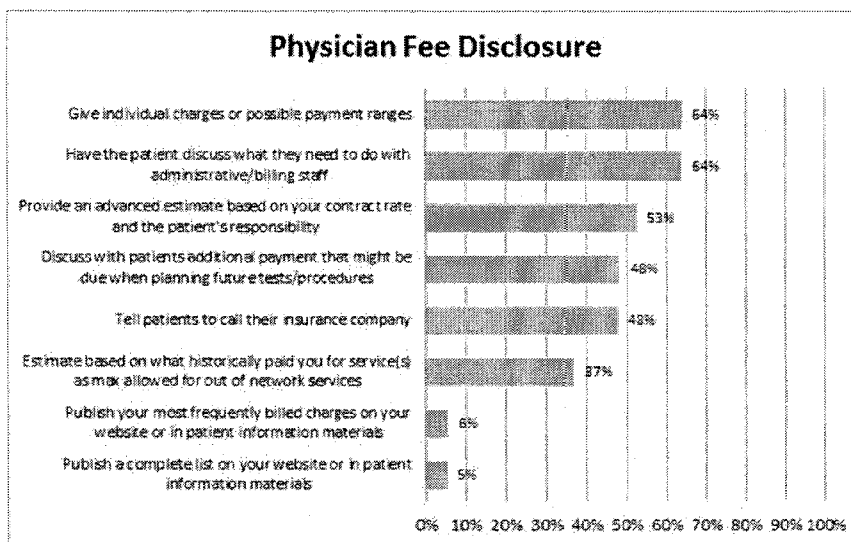
⁶⁸⁰ National Network of Libraries of Medicine, *supra* note 142.

⁶⁸¹ Senate Committee on State Affairs hearing, Sept. 15, 2014 (Testimony of Charles Bailey, Texas Hospital Association).

⁶⁸² Price Transparency in Healthcare, Report from the HFMA Price Transparency Task Force, Healthcare Financial Management Association (2014).

According to a report by HFMA, health plans should also alert patients to price information from out-of-network providers.⁶⁸³ If a patient seeks care from an out-of-network provider and contacts the health plan for assistance, the health plan should explain what percentage of the out-of-network charges the plan will cover.⁶⁸⁴ The health plan is also in the best position to inform the patient that, if the patient intentionally seeks care from an out-of-network provider, it is the patient's responsibility to independently obtain price information from that provider.⁶⁸⁵ Similarly, providers are the best source of price information for uninsured patients and patients seeking care from an out-of-network provider.

A recent 2014 Texas Medical Association (TMA) Physician Survey provided insight into how physicians communicate with patients about their fees. (See survey results below - note, physicians could choose from one or more of the disclosure methods).



Source: TMA Physician Survey 2014

Senate Bill 1731, 80th Legislature

In 2007, the 80th Texas Legislature passed Senate Bill 1731, an omnibus bill, that sought to increase transparency of multiple facets of the health care field.⁶⁸⁶ The law, among the most comprehensive in the country, promotes transparency and fair pricing in the health care industry. Senate Bill 1731, requires doctors and hospitals to create, maintain, and disclose to patients consistent billing practices that inform patients about the potentially high costs of out-of-network providers. The law also established a data reporting program to collect health plans' paid claims data from different service areas across the state to help consumers better understand costs and price variability.

⁶⁸³ Price Transparency in Healthcare, Report from the HFMA Price Transparency Task Force, Healthcare Financial Management Association (2014).

⁶⁸⁴ *Id.*

⁶⁸⁵ *Id.*

⁶⁸⁶ Acts 2007, 80th Leg., ch. 997.

The passage of Senate Bill 1731 provided patients, both insured and uninsured, the right to obtain health care estimates from hospitals, physicians, and health plans. The legislation recognized two groups of patients that will access services: the insured patient and the uninsured patient. The bill specifically delineated the two. The delineation was necessary, because the amount that will be paid out-of-pocket by the patient differs depending upon the insurance status of the patient. Additionally, the bill recognized that where a patient should seek information about what they will owe depends on whether or not the patient is insured.

As part of this reform, Senate Bill 1731 created the Texas Department of Insurance's (TDI) Consumer Reimbursement Rate Guide, which provides average regional health care prices for certain health care services based on claims data submitted by health insurers. Additionally, Senate Bill 1731 established an annual report card for health insurance companies that allow consumers to make direct comparisons of insurers' health plan benefits, costs, and quality. Most components of the legislation were implemented following its passage. In the past year, however, TDI has revisited the law's transparency goals.

Texas Department of Insurance

In September 2013, TDI partnered with the University of Texas School of Public Health (UTSPH) on a federal grant, which provided an opportunity to revisit TDI's health price transparency effort, evaluate progress to date, and make improvements to the Consumer Reimbursement Rate Guide.⁶⁸⁷ TDI is also working to implement health insurer report cards, an initiative that was previously suspended in order to avoid duplication with federal health reform requirements.⁶⁸⁸ TDI mostly relies on data insurers are already producing to comply with other state and federal requirements.

Health Price Transparency Grant

The objectives proposed under this grant are a continuation of previous efforts by Texas policymakers to promote a consumer-driven health care system and empower consumers with the information they need to make better health care decisions. Legislative efforts have given Texas consumers the right to request estimates from providers and health plans on prospective charges and negotiated prices before scheduling a procedure. Consumers can find the average prices negotiated by insurers within a region for 439 specific medical procedure codes on the Consumer Reimbursement Rate Guide established by TDI.⁶⁸⁹

Despite these strides, the complexity of health care pricing necessitates additional work to make price data more meaningful to consumers. Medical procedure codes make sense to medical billing specialists, but are less clear to the average consumer who cannot predict all of the components a provider may include on a bill for a given procedure. Through the work of the Texas Institute for Health Care Quality and Efficiency (the "Institute"), the challenges associated with price transparency have been discussed at length. The Institute recommends providing

⁶⁸⁷ Senate Committee on State Affairs hearing, Sept. 15, 2014 (Testimony of Katrina Daniel, Texas Department of Insurance).

⁶⁸⁸ See Appendix to Charge 7.

⁶⁸⁹ Senate Committee on State Affairs hearing, Sept. 15, 2014 (Testimony of Katrina Daniel, Texas Department of Insurance).

consumers with more timely cost estimates, encouraging health plans to provide enrollees with transparency tools, and endorsing the pursuit of voluntary participation by health insurers in a comprehensive claims database..⁶⁹⁰

TDI obtained a federal grant to support and enhance existing state efforts to provide transparency on the price of health care services through the Consumer Reimbursement Rate Guide..⁶⁹¹ TDI is pursuing activities under this grant in partnership with UTSPH..⁶⁹²

In addition to building on TDI's reimbursement rate data, this effort will utilize a database developed by UTSPH, which contains comprehensive claims data from Blue Cross Blue Shield of Texas, Texas Medicaid, and Medicare..⁶⁹³ The level of detail in this dataset will allow TDI to present pricing information in a format that is more reflective of a typical consumer experience..⁶⁹⁴ As additional private payers consider participating in this database, it provides a starting point for the research community to evaluate questions on a market-wide level.

Activities pursued under this grant will seek to enhance efficiency in the Texas healthcare marketplace by increasing price transparency and promoting best practices among insurers and providers. Primary approaches to achieving these objectives include:

- Connecting consumers to meaningful information on health care prices by:
 - Grouping medical procedure codes to illustrate the full cost of treatment the average consumer may face for a given procedure, including average prices for each component of the treatment and the treatment as a whole;
 - Identifying medical procedure codes associated with accepted treatment guidelines and giving consumers access to information on best practices for the treatment of certain conditions;
 - Analyzing pricing variation across geographic regions and service settings to identify trends and synthesize useful tips for consumers on avoiding high costs;
 - Improving the Consumer Reimbursement Rate Guide website to increase consumer understanding of the data it contains; and
 - Supporting voluntary insurer efforts to provide meaningful, contract-specific price information to enrollees in real time through an insurer-hosted web tool.

- Developing a comprehensive claims database to support research opportunities related to health care practices, payment methodologies, and health care utilization in Texas, managed by UTSPH in partnership with TDI to:
 - Encourage commercial carriers to share data for research without forfeiting the confidential status of proprietary data
 - Provide research opportunities in health economics, health policy, and health utilization management
 - Share analysis and findings with Texas leadership to inform policy decisions

⁶⁹⁰ See Appendix to Charge 7.

⁶⁹¹ Senate Committee on State Affairs hearing, Sept. 15, 2014 (Testimony of Katrina Daniel, Texas Department of Insurance).

⁶⁹² *Id.*

⁶⁹³ *Id.*

⁶⁹⁴ *Id.*

- Enhance TDI's ability to act as a resource for leadership on issues related to health care cost and utilization

TDI's Consumer Reimbursement Rate Guide

TDI's Consumer Reimbursement Rate Guide is an online tool that allows Texans to search for the average price for medical procedures in eleven regions statewide. The tool relies on data that TDI has collected since 2010 pursuant to TIC § 38.355 and TAC §§ 21.4501-4507. The existing tool is of limited use to consumers due to inherent limitations in the data call design, quality issues, and the format for presenting data.

TDI is working to address several challenges with collecting data..⁶⁹⁵ One challenge TDI faces is that collecting data at an aggregate level produces only one data point per issuer, which limits TDI's ability to evaluate whether data is reliable..⁶⁹⁶ Additionally, collecting only six months of data limits the number of claims that are included in the data issuers report..⁶⁹⁷ Finally, collecting data at the regional level limits the ability to reflect market-specific rates, because some regions include multiple metropolitan areas with different health care markets..⁶⁹⁸

UTSPH will analyze several technical issues with TDI's data collection processes and make recommendations for improvement. One issue UTSPH will analyze is that data in its current form does not allow TDI to report on the amount of variation in prices. Additionally, data is missing some necessary fields, such as "units of service." Finally the method for collecting data on inpatient and outpatient facility prices is overly simplified and does not account for the complexity involved in billing for services delivered in inpatient and outpatient facilities. One solution is to present pieces on treatment events, rather than individual billing codes. Another solution is to prioritize treatment events that are common, but also "shoppable."

TDI hosted a stakeholder meeting on April 15, 2014, to collect additional insight from consumers and the industry on how to address the remaining challenges and transform the Consumer Reimbursement Rate Guide into a useful tool for Texans.

Health Insurer Report Cards

Senate Bill 1731 established an annual report card for health insurance companies that allows consumers to make direct comparisons of insurers' health plan benefits, costs, and quality..⁶⁹⁹ Implementation was temporarily suspended in order to avoid duplication with federal health reform requirements, which include some transparency reporting requirements for health insurers. Recently, TDI began efforts to implement health insurer report cards by relying largely on data that insurers are already producing to comply with federal requirements..⁷⁰⁰

⁶⁹⁵ Senate Committee on State Affairs hearing, Sept. 15, 2014 (Testimony of Katrina Daniel, Texas Department of Insurance).

⁶⁹⁶ *Id.*

⁶⁹⁷ *Id.*

⁶⁹⁸ *Id.*

⁶⁹⁹ Acts 2007, 80th Leg., ch. 997.

⁷⁰⁰ See Appendix to Charge 7 (TDI's Efforts to Promote Transparency in Healthcare).

Transparency and the Balance Billing Problem

“Balance billing” occurs when a consumer receives out-of-network health care services and is directly billed by the provider for the balance of what the insurer did not pay.

Transparency and Emergency Room Billing

Most individuals will end up in the emergency room at some point, and when they do, they probably will not be able to choose which physician treats them and little or no ability to ensure the physician is part of the individuals' insurance company's network of preferred providers. Texas consumers also may reasonably assume that, if they are treated in an in-network hospital in an emergency, the physicians working in that hospital would also be in-network. However, that is often not the case and it can expose consumers surprise medical bills, or "balance bills," from out-of-network physicians.

In many cases, the physicians practicing in a hospital are not employees of the hospital and do not necessarily participate in the same insurance plans as the hospital. Hospitals commonly make arrangements with individual physicians or physician groups to provide medical services within the hospital. For example, a hospital may contract with one or more groups of emergency room physicians to provide services within the emergency room. Similar arrangements may be made with outside groups of doctors to provide anesthesiology, radiology, pathology, and neonatology services within the hospital. These groups of physicians, who are not hospital employees, decide independently which insurance plans to participate in and often do not participate in all of the same insurance plans that the hospital does. In practice, this means a trip to the emergency room can result in multiple separate bills from different providers and may result in a consumer receiving out-of-network physician services even if the consumer went to an in-network hospital.

Texas has some protections in place that lessen the impact of surprise bills stemming from emergency room visits, but these protections do not prohibit balance bills. According to a report by the Center for Public Policy Priorities (CPPP), a way to protect consumers in medical emergencies is to remove them from billing disputes between insurers and out-of-network providers.⁷⁰¹ CPPP suggests that the Texas Legislature remove consumers from the billing disputes by modifying Texas' successful, but tightly limited, balance-billing mediation process.⁷⁰²

Transparency and Balance Billing Outside the Emergency Room Context

Balance billing is not limited to emergency room situations. Consumers also receive unexpected balance bills following scheduled procedures, especially when out-of-network providers are brought in without the consumer's prior knowledge or consent. Even diligent consumers who ask many of the right questions leading up to an outpatient procedure report that they are unable to ensure that they will only be treated by in-network providers. For example, a consumer getting a

⁷⁰¹ See Appendix to Charge 7 (Stacey Pogue and Megan Randall, Surprise Medical Bills Take Advantage of Texans: Little-Known practice creates a "second emergency" for ER patients).

⁷⁰² See Appendix to Charge 7 (Stacey Pogue and Megan Randall, Surprise Medical Bills Take Advantage of Texans: Little-Known practice creates a "second emergency" for ER patients); see also Senate Committee on State Affairs hearing, Sept. 15, 2014 (testimony of Trey Berndt, AARP).

colonoscopy may ensure that their gastroenterologist and facility are in-network, but have an out-of-network anesthesiologist assigned at the last minute or have a biopsy sent off to an out-of-network pathologist that the consumer does not choose.

Is Transparency Enough

Meaningful transparency about network status of providers, out-of-network reimbursement methodologies, estimated charges, etc., are all important consumer protections and areas in which Texas has made significant progress. However, transparency alone does not prevent surprise balance bills, because consumers do not proactively or knowingly choose to get health care out-of-network in many cases. Even the most clear disclosure and data imaginable would be useless to a person suffering a stroke and being rushed to an emergency room. Furthermore, there are limits of transparency and disclosure even when consumers have access to information when they are not suffering medical emergencies. The current state of transparency and the efforts of Senate Bill 1731 are intended to help consumers minimize out-of-pocket costs. However, transparency will not work to eliminate balance billing altogether.

Recommendation

The Committee recommends that the Legislature continue to monitor medical price transparency and TDI's efforts and consider the impact of educating consumers on health care. Senate Bill 1731 will continue to provide information to consumers, regardless of insurance status, about what their out-of-pocket payment obligations are for health care services. Any legislative considerations should be beneficial and useful to consumers. Additionally, the Legislature should continue to study ways to lessen the impact of balance bills in the emergency room context or when consumers get care out-of-network involuntarily.

Charge No. 8

Monitor the actuarial and financial conditions of the pension and health care programs administered by the Teacher Retirement System (TRS) and the Employees Retirement System (ERS).

Actuarial and Financial Conditions of the Pension and Health Care Programs

The Employees Retirement System (ERS) was established in 1947 to provide retirement benefits to state employees. ERS administers four retirement funds.⁷⁰³ The general ERS fund serves state agency employees and elected state officials, including legislators, district attorneys, and statewide elected officials.⁷⁰⁴ The Law Enforcement and Custodial Officer Supplemental Retirement Fund (LECOSRF) provides supplemental benefits to state law enforcement officers commissioned by the Department of Public Safety, Texas Alcoholic Beverage Commission, Texas Department of Parks and Wildlife, Texas Facilities Commission, as well as certain custodial and parole officers employed by the Texas Department of Criminal Justice.⁷⁰⁵ Finally,

⁷⁰³ Employees Retirement System of Texas, *2014 Comprehensive Annual Financial Report* (Nov. 2014) file:///C:/Users/s1180bc/Downloads/2014CAFR.pdf

⁷⁰⁴ *Id.*

⁷⁰⁵ *Id.*

the Judicial Retirement System Plan I and Plan II provide benefits to judges and justices of the Supreme Court, Court of Criminal Appeals, Court of Appeals, and District Courts.⁷⁰⁶

As of August 31, 2014, the actuarial value of ERS Trust Fund was \$25.4 billion, and it returned 14.7 percent for fiscal year (FY) 2014.⁷⁰⁷ This return significantly outperformed both the actuarially assumed rate of return of eight percent and the actual thirty-year rate of return of 8.65 percent.⁷⁰⁸

Created in 1979 as a supplemental retirement benefit for ERS members who complete twenty or more years of service as commissioned law enforcement officers, LECOSRF currently provides supplemental benefits to 10,024 retirees and beneficiaries.⁷⁰⁹ The actuarial value of assets is \$884 million.⁷¹⁰ With accrued liabilities of \$1.207 billion the fund currently has an unfunded liability of \$323 million.⁷¹¹ The result is a funded ratio of 73.2 percent.⁷¹² In FY 2014, the actuarially sound contribution rate was 3.09 percent, but the actual combined contribution rate by law enforcement employees, court fees, and the state was 2.20 percent, leaving a shortfall of 0.89 percent.⁷¹³

Judges and justices appointed or elected prior to September 1, 1985, receive their retirement benefits through the Judicial Retirement System Plan I (JRS I), which had an unfunded actuarial accrued liability of \$245.4 million as of the end of the 2014 fiscal year.⁷¹⁴ JRS I is a pay-as-you-go plan and is not pre-funded.⁷¹⁵ Instead, active members contribute a portion of their salary to the program during their first twenty years of service and may elect to continue contributing to accrue additional benefits.⁷¹⁶ In FY 2014, active members contributed 6.6 percent of their salaries.⁷¹⁷ The contribution rate will increase to 6.9 percent in FY 2015, 7.2 percent in FY 2016, and 7.5 percent in FY 2017.⁷¹⁸ The state contributes all additional revenue necessary to cover ongoing costs of retirees.⁷¹⁹ At the end of FY 2014, there were 12 active members in JRS I.⁷²⁰

All judges and justices who took office after August 31, 1985, receive their retirement benefits through the Judicial Retirement System Plan II (JRS II). As of August 31, 2014, JRS II had a funding ratio of 90.2 percent, with actuarially valued assets of \$348.4 million and an unfunded

⁷⁰⁶ Employees Retirement System of Texas, *2014 Comprehensive Annual Financial Report* (Nov. 2014) file:///C:/Users/s1180bc/Downloads/2014CAFR.pdf

⁷⁰⁷ Employees Retirement System of Texas, *2014 Annual Investment Summary* (Nov. 2014) http://www.ers.state.tx.us/About_ERS/Investments/Performance/

⁷⁰⁸ *Id.*

⁷⁰⁹ Employees Retirement System of Texas, *Actuarial Valuation Reports for Pension Plans Administered by ERS* (Dec. 2014) file:///C:/Users/s1180bc/Downloads/2014_ERS_Pension_Plan_Valuations.pdf

⁷¹⁰ *Id.*

⁷¹¹ *Id.*

⁷¹² *Id.*

⁷¹³ *Id.*

⁷¹⁴ *Id.*

⁷¹⁵ *Id.*

⁷¹⁶ *Id.*

⁷¹⁷ *Id.*

⁷¹⁸ *Id.*

⁷¹⁹ *Id.*

⁷²⁰ *Id.*

actuarial accrued liability of 37.85 million.⁷²¹ As with JRS I, active members contribute a portion of their salary to the program during their first twenty years of service and may elect to continue contributing to accrue additional benefits.⁷²² In FY 2014, active members contributed 6.6 percent of their salaries.⁷²³ The contribution rate will increase to 6.9 percent in FY 2015, 7.2 percent in FY 2016, and 7.5 percent in FY 2017.⁷²⁴ In FY 2014, the actuarially sound contribution rate for JRS II was 24.08 percent, but the actual combined contribution rate by judicial employees and the state was 22.23 percent, leaving a shortfall of 1.85 percent.⁷²⁵

The Employees Retirement System Group Benefit Program (ERS-GBP) provides Health insurance to state employees, retirees, and their eligible dependents.⁷²⁶ Today, 520,772 people participate in ERS-GBP.⁷²⁷ All participants receive access to the same benefits and coverage and are subject to the same contribution structure.

Currently, ERS-GBP offers three major options for health coverage. HealthSelect, a self-funded, point-of-service plan is by far the largest.⁷²⁸ With 436,081 participants, this plan includes 84.1 percent of the GBP's covered lives.⁷²⁹ HealthSelect is administered by UnitedHealthcare and provides both in-network and out-of-network benefits. Pharmacy benefits for the plan are administered by Caremark.

The second option offered under ERS-GBP includes two regional Health Maintenance Organizations (HMOs). These HMOs provides health coverage and prescription drug benefits to HMO participants and their eligible dependents in fifty-two Texas counties. Current HMO providers are Community First Health Plans, Inc. and Scott & White Health Plan. This coverage is provided through contracts with private HMOs in the Community First or Scott & White service areas. Approximately 24,627, or 4.75 percent of GBP participants, are enrolled in one of the HMO options.⁷³⁰ To be selected, an HMO must be able to provide benefits in each proposed service area at a lower cost than can otherwise be provided through the self-funded plan.

The third option is offered under Medicare Advantage, an HMO and preferred provider organization (PPO) plan, which provides health coverage to Medicare-enrolled retirees, surviving spouses, and their dependents. Medicare-eligible retirees are automatically enrolled in Medicare Advantage, and there are 57,263 participants, or 11.05 percent of GBP participants, enrolled in the plan.⁷³¹

⁷²¹ Employees Retirement System of Texas, *Actuarial Valuation Reports for Pension Plans Administered by ERS* (Dec. 2014) file:///C:/Users/s1180bc/Downloads/2014_ERS_Pension_Plan_Valuations.pdf

⁷²² *Id.*

⁷²³ Employees Retirement System of Texas, *Actuarial Valuation Reports for Pension Plans Administered by ERS* (Dec. 2014) file:///C:/Users/s1180bc/Downloads/2014_ERS_Pension_Plan_Valuations.pdf

⁷²⁴ *Id.*

⁷²⁵ *Id.*

⁷²⁶ Acts 1975, 64th Leg., Ch. 79.

⁷²⁷ Senate Committee on State Affairs hearing, Dec. 9, 2014 (Written testimony of Ann Bishop, Employees Retirement System of Texas).

⁷²⁸ *Id.*

⁷²⁹ *Id.*

⁷³⁰ *Id.*

⁷³¹ *Id.*

Funding needs for the ERS-GBP are calculated biennially based on anticipated claims costs and the contribution levels necessary to cover those costs. With the State covering 100 percent of the cost of employee and retiree coverage and fifty percent of the cost of spouse and dependent coverage, funding requests are then estimated based on predicted participation in the program. For the 2014-2015 biennium, ERS projects a need to increase biennial funding by 6.9 percent (\$190.5 million in general revenue) to maintain the same level of benefits..⁷³²

As part of its 2016-2017 Legislative Appropriation Request (LAR), ERS has projected a plan cost trend of 8.5 percent for FY 2016-2017..⁷³³ The base request calculation required by the Legislative Budget Board (LBB) looks exclusively at the FY 2015 levels.

The Teacher Retirement System (TRS) was established in 1937, and provides retirement benefits to employees of public school districts and institutions of higher education..⁷³⁴ TRS serves 1.4 million active and retired members, which is one out of every twenty Texans..⁷³⁵ As of August 2014, the market value of the TRS pension fund was \$132.2 billion and earned a rate of return of 16.9 percent for FY 2014..⁷³⁶ This return significantly outperformed the actuarially assumed rate of return of eight percent..⁷³⁷ The average monthly retirement payment out of the fund is \$1,995, and TRS paid \$8.5 billion in retirement benefits in FY 2014..⁷³⁸

During the 83rd Regular Session of the Texas Legislature, statutory changes were made to the TRS pension fund by the enactment of Senate Bill 1458..⁷³⁹ That bill made changes to the law that will gradually increase member contributions to 7.7 percent in 2017..⁷⁴⁰ The bill also requires school districts that do not pay the Social Security payroll tax to contribute 1.5 percent of payroll that would be subject to the payroll tax..⁷⁴¹ According to the Social Security Administration, salaried amounts up to \$117,000 in 2014 and \$118,500 in 2015 are subject to the tax..⁷⁴² Furthermore, the bill increased the minimum retirement age with full pension benefits to age 62 for all non-vested members (those with less than five years of service credit as of August 31, 2014)..⁷⁴³ All vested members as of that date are grandfathered..⁷⁴⁴ Lastly, the bill set a minimum age of 62 to receive TRS-Care 2 or TRS-Care 3 (health care plans for retirees)..^{745 746}

⁷³² Senate Committee on State Affairs hearing, Dec. 9, 2014 (Written testimony of Ann Bishop, Employees Retirement System of Texas).

⁷³³ *Id.*

⁷³⁴ Senate Committee on State Affairs hearing, Dec. 9, 2014 (See generally written testimony of representatives of the Teacher Retirement System).

⁷³⁵ *Id.*

⁷³⁶ *Id.*

⁷³⁷ *Id.*

⁷³⁸ *Id.*

⁷³⁹ S.B. 1458, 83rd Leg., Regular Sess. (Tex. 2013) (enacted).

⁷⁴⁰ *Id.*

⁷⁴¹ *Id.*

⁷⁴² Social Security Administration, *Benefits Planner: Maximum Taxable Earnings (1937 - 2015)*, <http://www.ssa.gov/planners/maxtax.htm> (last visited Dec. 14, 2014).

⁷⁴³ S.B. 1458, 83rd Leg., Regular Sess. (Tex. 2013) (enacted).

⁷⁴⁴ *Id.*

⁷⁴⁵ *Id.*

As a result of these changes, increased contributions, and high investment returns, the TRS pension fund is actuarially sound, which allowed the 83rd Legislature to provide a benefit enhancement (i.e. cost of living adjustment) of three percent (capped at \$100 per month) to members who retired on or before August 31, 2004..⁷⁴⁷

TRS administers health care programs for both active members and retirees..⁷⁴⁸ Created in 1985, TRS-Care is the health care program for retired members..⁷⁴⁹ The program offers a basic health care plan at no cost, as is required by Chapter 1575 of the Insurance Code, and other optional plans, such as coverage for coverage for spouses and eligible dependents..⁷⁵⁰ TRS-Care currently offers three plan options..⁷⁵¹ TRS-Care 1 is the basic plan and provides catastrophic coverage..⁷⁵² TRS-Care 2 and TRS-Care 3 offer more comprehensive benefits, including a prescription drug benefit..⁷⁵³ As of August 31, 2014, there were 29,996 members enrolled in TRS-Care 1, 56,210 members enrolled in TRS-Care 2, and 158,362 members enrolled in TRS-Care 3..⁷⁵⁴

TRS-Care is funded by investment income, a Medicare Part D drug subsidy, member premiums, and contributions by the state, school district, and active school employees..⁷⁵⁵ The state contributes one percent of active member payroll, while each school district contributes 0.55 percent and active school employees 0.65 percent..⁷⁵⁶ Despite these funding sources, a shortfall of \$727 million is expected for the program during the 2016-2017 fiscal biennium..⁷⁵⁷ In the past, the state has made supplemental appropriations to cover previous shortfalls. From FY 2001 to FY 2005, for example, the state made supplemental appropriations of \$849 million..⁷⁵⁸ A study of TRS-Care presented several options for the Legislature to consider in addressing the shortfall..⁷⁵⁹ Those options included pre-funding the long-term liability of the program, funding on a pay-as-you-go basis, funding for a 10-year solvency, requiring retirees pay the full cost of optional coverage, requiring the purchase of Medicare Part B, transitioning the program to fixed contribution vouchers, creating a consumer-directed plan for the non-Medicare population, or a combination thereof..⁷⁶⁰

⁷⁴⁶ Members are grandfathered if the sum of the person's age and amount of service credit in the retirement system equals 70 or greater; or the person has at least 25 years of service credit in the retirement system as of August 31, 2014. All non-grandfathered individuals will only be eligible to receive TRS-Care 1 until they reach age 62. Current retirees are not affected.

⁷⁴⁷ Senate Committee on State Affairs hearing, Dec. 9, 2014 (See generally written testimony of representatives of the Teacher Retirement System).

⁷⁴⁸ *Id.*

⁷⁴⁹ *Id.*

⁷⁵⁰ *Id.*

⁷⁵¹ *Id.*

⁷⁵² *Id.*

⁷⁵³ *Id.*

⁷⁵⁴ *Id.*

⁷⁵⁵ *Id.*

⁷⁵⁶ *Id.*

⁷⁵⁷ *Id.*

⁷⁵⁸ *Id.*

⁷⁵⁹ *Id.*

⁷⁶⁰ *Id.*

TRS-ActiveCare was created in 2001 and went into effect on September 1, 2002.⁷⁶¹ Originally, it was intended for small school districts, but since its creation most large school districts have chosen to join the program.⁷⁶² Once a school district chooses to join, it cannot opt-out.⁷⁶³ TRS-ActiveCare offers four self-funded plans administered by Aetna: Active-Care 1, ActiveCare 1-HD, ActiveCare Select, and ActiveCare 2.⁷⁶⁴ Three fully-insured regional health maintenance organizations (HMOs) are also offered within certain service areas: FirstCare, Scott & White, and Allegian.⁷⁶⁵ As of August 31, 2014, there were 188,945 members enrolled in ActiveCare 1 and ActiveCare 1-HD, 169,086 members enrolled in ActiveCare 2, 73,816 members enrolled in ActiveCare Select, and 50,837 members enrolled with one of the HMOs.⁷⁶⁶

TRS-ActiveCare is funded by a \$75 monthly contribution from the state, a \$150 minimum contribution from the school district, and active employee premiums.⁷⁶⁷ The state contribution level has remained the same since TRS-ActiveCare went into effect in 2002.⁷⁶⁸ Since 2003, there have been eight premium increases, ranging from approximately five percent in 2003-2004 to as high as twenty-five percent for some plans in 2013-2014.⁷⁶⁹ Premium increases of up to eight percent are again expected for 2015.⁷⁷⁰ A study of TRS-ActiveCare presented several options that the Legislature may consider, such as returning funding ratios and benefits back to FY 2003 levels, allowing health savings accounts (HSAs), self-funding an Exclusive Provider Organization (EPO), eliminating uniform statewide coverage, eliminating coverage for spouses, or a combination thereof.⁷⁷¹

Recommendation

The Committee recommends that the Legislature continue to monitor the financial conditions of the pension and health care programs administered by the Teacher Retirement System and the Employees Retirement System, and, where necessary, take actions to ensure the affordability and sustainability of those programs.

Charge No. 9

Monitor the implementation of legislation addressed by the Senate Committee on State Affairs, 83rd Legislature, and make recommendations for any legislation needed to improve, enhance, and/or complete implementation.

The Committee took no action relating to this charge.

⁷⁶¹ Senate Committee on State Affairs hearing, Dec. 9, 2014 (See generally written testimony of representatives of the Teacher Retirement System).

⁷⁶² *Id.*

⁷⁶³ *Id.*

⁷⁶⁴ *Id.*

⁷⁶⁵ *Id.*

⁷⁶⁶ *Id.*

⁷⁶⁷ *Id.*

⁷⁶⁸ *Id.*

⁷⁶⁹ *Id.*

⁷⁷⁰ *Id.*

⁷⁷¹ *Id.*

Charge No. 10

Study and make recommendations relative to the structure of Texas Mutual Insurance Company and the residual market for workers' compensation insurance in Texas.

Background

In the 1980s, the Texas workers' compensation system declined rapidly. Medical costs were higher than in other states and were increasing at a much higher rate than medical costs outside the workers' compensation system. Although state-promulgated rates more than doubled from 1984 to 1989, Texas insurers were still losing money and carriers began reducing the number of policies they would write. Several major insurers threatened to leave the state and many employers were forced to purchase insurance from the state's assigned risk pool, insurer of last resort. In the 1980s, workers' compensation insurers were required to pay more than \$1.5 billion to cover the pool's losses. Business groups claimed that spiraling costs forced large businesses to locate operations elsewhere and forced small businesses to cease operations or go without coverage. In 1987, the Legislature appointed a Joint Select Committee on Workers' Compensation. The committee's report served as the initial roadmap for recovery and formed the basis of the first significant reforms.

In 1991, as part of a major overhaul of the Texas workers' compensation system, the Legislature created the Texas Workers' Compensation Insurance Fund (the "Fund") to serve as a provider of last resort for the workers' compensation market for businesses that were unable to find coverage elsewhere.⁷⁷² The Fund was initially capitalized through the sale of \$300 million in revenue bonds, which established the initial surplus and reserves, and paid costs related to the bonds. The state transferred \$5 million to Fund as a working capital loan. The Fund repaid the loan in the first year with interest, and it repaid all of the bonds by 1999.⁷⁷³

In 2001, the Legislature changed the name of the Fund to the Texas Mutual Insurance Company ("Texas Mutual") and authorized it to operate as a domestic mutual insurance company owned by its employer policyholders.⁷⁷⁴ Among other provisions, it reduced the number of gubernatorial appointees on the board of directors from nine to five, removed the company from Sunset Review, and eliminated the Attorney general's oversight.⁷⁷⁵

Hearing

The Committee held a public meeting and received testimony for Charge No. 10 on September 15, 2014.

Recommendation

The Committee makes no recommendation.

⁷⁷² Acts 1991, 72nd 2nd C.S., ch. 12, General and Special Laws of Texas.

⁷⁷³ See Appendix to Charge 10 (Significant Legislation and Events Affecting Texas Mutual Insurance Company).

⁷⁷⁴ Acts 2001, 77th R.S., ch. 1195, General and Special Laws of Texas.

⁷⁷⁵ *Id.*



APPENDIX TO CHARGE 1



February 24, 2014

PRESIDENT
J.B. Van Hollen
Wisconsin Attorney General

PRESIDENT-ELECT
Jim Hood
Mississippi Attorney General

VICE PRESIDENT
Marty Jackley
South Dakota Attorney General

IMMEDIATE PAST PRESIDENT
Douglas Gansler
Maryland Attorney General

EXECUTIVE DIRECTOR
James McPherson

The Honorable Patrick Leahy
Chairman, Committee on the Judiciary
United States Senate
224 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable John D. Rockefeller IV
Chairman, Committee on Commerce,
Science and Transportation
United States Senate
254 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Chuck Grassley
Ranking Member, Committee on the
Judiciary
United States Senate
224 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable John Thune
Ranking Member, Committee on
Commerce, Science and Transportation
United States Senate
254 Russell Senate Office Building
Washington, D.C. 20510

Dear Chairman Leahy, Ranking Member Grassley, Chairman Rockefeller, and
Ranking Member Thune:

We, the Attorneys General of 42 states,¹ write to express our support of your efforts to enact bipartisan patent reform legislation, and to share our concerns with the currently proposed S. 1720 and the recently passed H.R. 3309. So-called patent trolls stifle innovation and harm our economy by making dubious claims of patent infringement and using the threat of expensive litigation to extort money from small businesses and nonprofits. We have received many complaints from these businesses and nonprofits, our constituents, who are desperate for relief from the misuse of the patent system. While these threats were once focused on tech businesses, they are now levied at all manner of businesses, including banks, hospitals, restaurants and hotels.

Our offices have responded to these complaints by launching investigations and bringing enforcement actions against patent trolls, which have threatened thousands of businesses and non-profits for their use of common, everyday technology such as scanners and Wi-Fi networks. Our authority to protect businesses derives primarily from state statutes that prohibit unfair and deceptive acts. Though any patent holder has a right to fight infringement, it may not do so in a manner that is unfair or deceptive.

We are encouraged by your attempts to enact patent reform, but would like Congress to consider amendments to address the following:

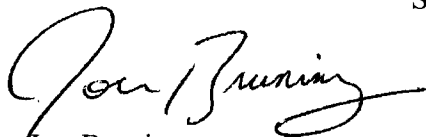
¹ Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut, Florida, Guam, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Mexico, New York, North Carolina, North Dakota, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, and Wyoming.

2030 M Street, NW
Eighth Floor
Washington, DC 20036
Phone: (202) 326-6000
<http://www.naag.org/>

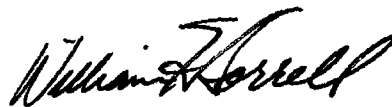
1. **Confirmation of state enforcement authority.** We support the provision in S. 1720 which expressly prohibits unfair and deceptive demand letters and would clarify the Federal Trade Commission's authority to prohibit bad-faith demand letters. However, federal legislation should also confirm the concurrent authority of state attorneys general to bring the same types of enforcement actions under state law. State attorneys general work closely with the FTC on many consumer protection matters and generally have the same authority to protect consumers and bring enforcement actions. In many states, the interpretation of state law and its enforcement expressly track federal law. H.R. 3309's study on demand letters is important to understanding what is occurring, but a study by itself does not provide adequate, timely relief for the serious problem that small businesses around the country currently face – the threat of immediate litigation for failing to pay often unfounded and exorbitant licensing fees.
2. **Clarification of state-court jurisdiction over bad-faith demand letters.** Patent trolls typically argue that sending demand letters into a state – even misleading or deceptive demand letters – is insufficient to support a finding of personal jurisdiction in the courts of that state. That argument is flatly inconsistent with longstanding interpretations of state consumer protection laws and the due process requirements for actions brought under those laws. Federal legislation should confirm that state courts have personal jurisdiction over entities that direct unfair or deceptive patent demand letters into the state.
3. **Transparency for patentees that send demand letters.** We support any efforts to increase transparency in the patent enforcement process, as sunlight and transparency may deter the worst abusers of our patent laws. However, the key transparency provisions in S. 1720 and H.R. 3309 apply only when a patentee files a civil action alleging infringement. That is too late. Patent trolls often succeed in extracting licensing fees and settlements before any litigation is filed. Instead, disclosure should be required of all those with a financial interest in the patent at the time a patent demand letter is sent.
4. **Patent litigation reform.** One reason that the patent troll business model is successful is that the cost of patent litigation usually far outstrips the cost of a settlement. Though our focus is primarily on addressing patent trolling from a consumer protection standpoint, often centering on demand letters, we recognize the importance of pending Congressional legislation on this issue. We are generally supportive of structural federal patent litigation reform which would create an environment in which abusers of the patent enforcement system cannot thrive.

Again, thank you for your continuing leadership in maintaining the quality and effectiveness of our patent system. We look forward to working with you in the effort to deter the bad actors who are exploiting the system for undeserved gain.

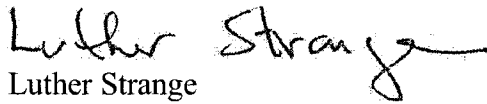
Sincerely,



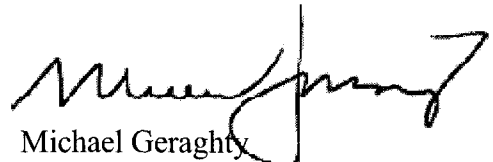
Jon Bruning
Nebraska Attorney General



William H. Sorrell
Vermont Attorney General



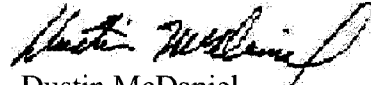
Luther Strange
Alabama Attorney General



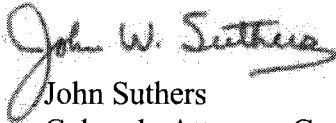
Michael Geraghty
Alaska Attorney General



Tom Horne
Arizona Attorney General



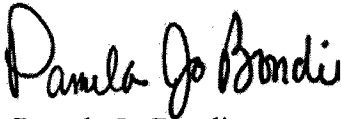
Dustin McDaniel
Arkansas Attorney General



John Suthers
Colorado Attorney General



George Jepsen
Connecticut Attorney General



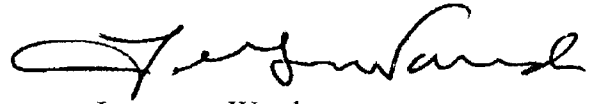
Pamela Jo Bondi
Florida Attorney General



Lenny Rapadas
Guam Attorney General



David Louie
Hawaii Attorney General




Lawrence Wasden
Idaho Attorney General



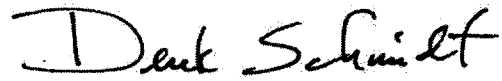
Lisa Madigan
Illinois Attorney General



Greg Zoeller
Indiana Attorney General



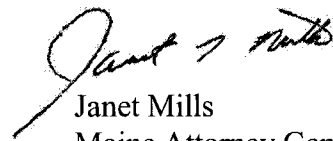
Tom Miller
Iowa Attorney General



Derek Schmidt
Kansas Attorney General



James "Buddy" Caldwell
Louisiana Attorney General



Janet Mills
Maine Attorney General



Douglas F. Gansler
Maryland Attorney General



Martha Coakley
Massachusetts Attorney General

Bill Schuette
Michigan Attorney General

Jim Hood
Mississippi Attorney General

Timothy Fox
Montana Attorney General

Joseph Foster
New Hampshire Attorney General

Eric T. Schneiderman
New York Attorney General

Wayne Stenehjem
North Dakota Attorney General

Kathleen Kane
Pennsylvania Attorney General

Alan Wilson
South Carolina Attorney General

Robert E. Cooper, Jr.
Tennessee Attorney General

Lori Swanson
Minnesota Attorney General

Chris Koster
Missouri Attorney General

Catherine Cortez Masto
Nevada Attorney General

Gary King
New Mexico Attorney General

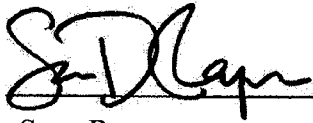
Roy Cooper
North Carolina Attorney General

Ellen Rosenblum
Oregon Attorney General

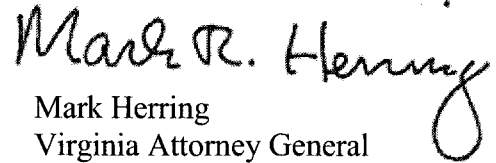
Peter Kilmartin
Rhode Island Attorney General

Marty J. Jackley
South Dakota Attorney General

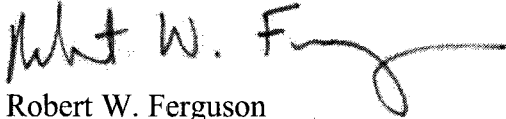
Greg Abbott
Texas Attorney General



Sean Reyes
Utah Attorney General



Mark Herring
Virginia Attorney General



Robert W. Ferguson
Washington Attorney General



Peter K. Michael
Wyoming Attorney General

Copy: The Honorable Harry Reid, Majority Leader, United States Senate
The Honorable Mitch McConnell, Minority Leader, United States Senate

Caterpillar Inc.
Testimony
Senate State Affairs Committee
Monday, September 15, 2014 at 8:00 A.M.
Capitol Extension, Room E.012

Good afternoon, Mr. Chairman, Members of the Committee:

For the record, my name is Kathy Barber, State Governmental Affairs for Caterpillar Inc.

Caterpillar Inc. is proud to have a large investment here in Texas and appreciate the opportunity to discuss the patent system and how Caterpillar operates within that system.

Caterpillar has more than fourteen thousand patents worldwide - either awarded or in the approval process. We are a company of innovation - we spend \$8 million a day on R&D.

We acknowledge that bad-faith demand letters are a problem. Caterpillar is sympathetic to the issue as we also have been recipients of these so-called "patent trolling practices." At the same time, however, we also need the ability to protect our hard-earned patents. We need the right – without violating the law – to send letters in good faith to those who may be infringing our patents.

There is a distinct and critically important difference between false and misleading written communications sent by certain patent assertion entities, and those patent holders who communicate in good faith, which include small start-ups and large companies alike, as well as individual inventors and universities. Patent assertion entities mass mail letters to small businesses, retailers and banks hoping to "score" settlements based solely on intimidation through false or misleading statements. Valid patent holders communicate in good faith to the public regarding their patent portfolio including offering their patents for license, and when necessary, protecting their patented products from being infringed.

In many instances the primary goal of the good faith sender of any written communication concerning their patented technology is simply to prevent copying and ensure product differentiation within an industry. This is best accomplished by providing early notice, before moneys are committed to substantial design and manufacturing investment, so that "design-arounds" are more readily accomplished. Recipients take these letters seriously in the design and development of new products and technology to avoid knowingly infringing on another's patent rights.

Legitimate patent demand communications serve an important role in advancing technologies, providing consumers more choices and ensuring the efficient self-policing of patent rights as well as preventing patent suits before they happen.

We believe legislation on patent demand communications should address three areas of concern:

(1) sanctions should be limited to those who send false and misleading written patent demand letters in bad faith to large populations of end users to extort settlements – routine business-to-business communications should not be swept-in;

(2) clear "rules of the road" with guidance as to what such communications should and should not contain - not a list of vague and subjective good faith and bad faith factors for a court to weigh in determining what constitutes a bad faith patent demand letter – this provides no real guidance to the sender as to what constitutes a legitimate written patent communication; and,

(3) a "safe harbor" should be provided that clearly states what all patent owners in good faith remain free to do. An appropriately crafted safe harbor will also help to insulate any legislation from federal patent law preemption or challenge on Constitutional grounds as intruding on protected free speech.

I would urge this committee to carefully consider any future legislation regarding written patent demand letters to ensure it does not interfere with legal business-to-business communication and inadvertently chill legitimate patent communications.

I also would encourage the legislature to forego a private cause of action and authorize the Attorney General to act as a "clearing house" or aggregator of complaints regarding patent assertion entities. This would allow end-users who have received threatening letters for patent infringement to file complaints with the Attorney General who can then identify patterns of abuse by the sender and pursue legal action against bad actors.

In closing, this issue is a moving target and thoughtful consideration must be given to any future proposals to ensure legitimate business-to-business communications are not interrupted by unintended consequences of state legislation.

APPENDIX TO CHARGE 2

APPENDIX TO CHARGE 3

APPENDIX TO CHARGE 4

APPENDIX TO CHARGE 5

GRANICUS Video streaming

Overview

The legislature recently converted its video streaming from Real Player to Granicus of live and archived sessions for both the Chambers and Committees. Video streaming in the senate has been available since 1999.

Real Player

When the legislature was using Real Player for video streaming, there was:

- Limited bandwidth capacity
- Limited picture quality for public live stream and archives
- Multiple bit rates of the streaming depending on where you were connecting:
 - Capitol - 220K
 - District Office - 80K
 - Public - 80K
 - Mobile devices - 150K
 - Archives - 34K
- No mobile capability to view archived files
- Real Player required users to download a specific player agent to view the video stream

Granicus

With Granicus, the legislature has a more robust and flexible video infrastructure that provides better quality live streaming and archived video for the Capitol and public.

Immediate benefits to the new streaming service include:

- Unlimited bandwidth capacity
- Unlimited storage capacity
- Higher picture quality in live streaming and archives
- A single, higher bit rate of 350K for Capitol, District Office, Public, Mobile and Archive streams
- Ability to view video archives on mobile devices
- Growth capability for indexing archive video streams
- No specific player agent is required in order to view the video streams

Senate Witness Registration System Pilot

System Overview

The Senate Witness Registration System (SWRS) automates the witness registration process, the processing of witness testimony during a hearing, and the production of the Meeting Witness List. SWRS is currently in a pilot phase with volunteer committees. If adopted, the use of SWRS will be optional for each senate committee, as determined by the chair of the committee. Since the use of SWRS would be optional, committees can determine on a committee hearing basis whether to use SWRS or hard copy witness cards to register witnesses.

There are three main components of the SWRS:

Witness Registration

- There are iPad kiosk stations within the extension to collect electronic witness registrations while a witness is onsite at the Capitol.
- For committees choosing to use SWRS, the kiosks will list hearings currently accepting electronic registrations.
- Witnesses may use their own mobile devices to access the registration website, if they're onsite and connected to the Capitol's public Wi-Fi network.
- Rolling kiosks will also be available for hearings held in the Betty King Room, the Senate Chamber or any other designated meeting room.
- In order to speed registration, witnesses may create personal registration accounts that contain the contact information required for each individual witness registration.

Clerk System

- The Senate Committee System provides clerks with the ability to create registration agendas for the kiosks, to display the current witness on the committee member's iPads, sort witnesses as requested by the chair, process witness testimony during a hearing, and capture information about the testimony delivered.
- After the hearing, the electronic registrations submitted by witnesses are then used to produce the Meeting Witness List.

Committee Member System

- During a hearing, an internal, secured webpage is available on an iPad for all committee members and designated staff to view the current witness information and the witnesses who have previously testified on that measure.
- There is also a secured Chair view that allows chairs to see all witness registration information - current witness, previous witnesses, and all upcoming witnesses.

APPENDIX TO CHARGE 6



2013 Annual Report

HISTORY AND PURPOSE: The Texas Health Insurance Pool was created by the Texas Legislature to provide health insurance to eligible Texas residents with preexisting medical conditions who were unable to obtain coverage from commercial insurers. As required by the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Pool also served as the Texas alternative mechanism for individual health insurance coverage, guaranteeing portability of coverage to qualified individuals who lost coverage under a U.S. employer-based plan. The Pool began issuing coverage January 1998 and provided health benefits to more than 95,000 Texans.

ADMINISTRATION: The Pool is governed by a nine-member Board of Directors, appointed by the Texas Commissioner of Insurance. The selected Board members represent diverse interests, including insurance consumers, insurance companies, health care providers, and insurance agents. The Board's activities are supported by a full-time Executive Director who oversees the day-to-day operations of the program.

BOARD OF DIRECTORS

D. Gregory Barbutti, Secretary/Treasurer
Consumer Representative (1997)

Gary C. Cole, Board Chair
Public Representative (1997)

Robert H. Emmick, Jr., M.D.
Professional Representative (1997)

Pati McCandless
Insurance Industry Representative (2003)

Maureen Milligan, Ph.D.
Public Representative (2011)

Richard C. Ott, CLU, LUTCF, Board Vice-Chair
Insurance Agent Representative (1999)

Victoria Paparelli, APRN
Professional Representative (2007)

William C. Rainey, M.D. (Term ended 9/1/13)
Consumer Representative (2002)

Marinan Williams
Insurance Industry Representative (2007)

POOL MANAGEMENT

Texas Health Insurance Pool
F.O. Box 17463
San Antonio, TX 78217
Phone: (512) 963-4990
Steven Browning, Executive Director

Customer Service: (888) 398-3927
Email: poolinfo@txhealthpool.org
Web: www.txhealthpool.org

2013 PROGRAM HIGHLIGHTS

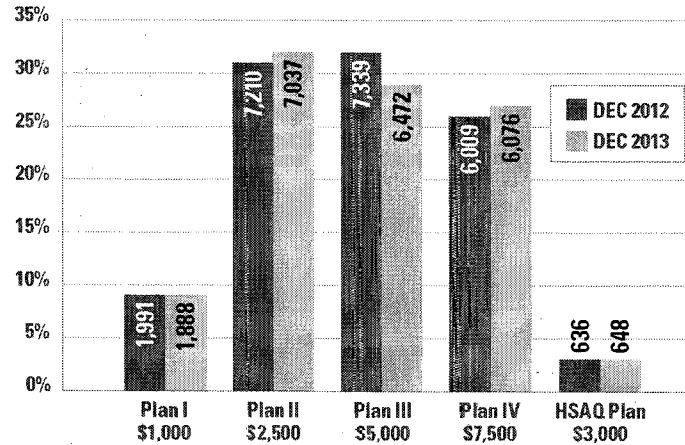
- **Legislative Activities:** S.B. No. 1367, passed during the 83rd regular session of the Texas Legislature, authorized the commissioner of insurance to determine the date of Pool coverage termination and directed the Pool Board to develop a plan for dissolving the Pool.
- **Policyholder Education/Outreach:** During 2013, the Pool implemented a comprehensive campaign to educate policyholders about the new health insurance marketplace and ensure that all were fully aware that their Pool coverage would end March 31, 2014.
- **Low-Income Premium Subsidy Program:** In 2009, the Texas Legislature created a premium assistance program for lower-income Pool policyholders, funded by a share of the penalties paid by insurers and HMOs to medical providers for late-paid clean claims. During 2013, this program reduced premiums for ± 4,400 Pool policyholders by a total of ±\$12.1 million. The average monthly premium reduction was ±\$300 per recipient. S.B. No. 1367 also authorized the commissioner of insurance to redirect the penalty funds, once no longer needed by Pool members.
- **Federal Grants/Premiums:** The Pool secured supplemental federal grant funding that reduced policyholder premiums by 5.1%.
- **Cost Containment:** The Pool's various cost containment programs (disease and case management, pharmacy clinical programs, audits and subrogation) reduced claim costs by ±\$30 million.
- **Network Discounts:** The medical and pharmacy networks leased from Blue Cross and Blue Shield of Texas and Express Scripts eliminated ±\$449 million in charges billed to Pool policyholders.

ELIGIBILITY: In 2013, Texas residents under age 65 qualified for the Pool if they could document at least one of the following specific eligibility criteria established by statute:

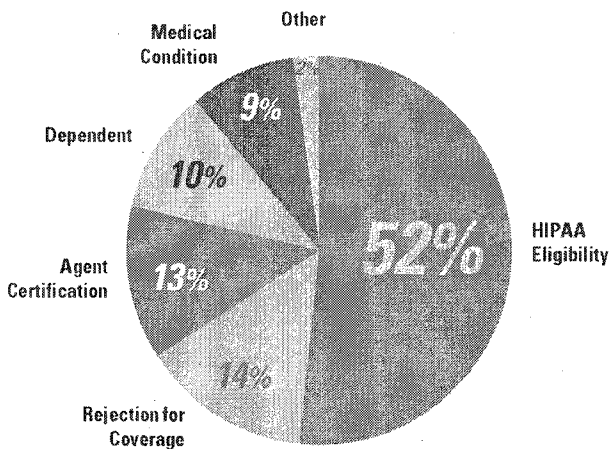
- At least 18 months of previous health insurance coverage, with no gap in coverage greater than 63 days, and the most recent coverage through a health plan provided by a U.S. private employer, church or governmental entity. This is known as federal HIPAA eligibility.
- Rejection or refusal by an insurer to issue substantially similar individual health insurance, due to health reasons.
- Offer by an insurer to issue substantially similar individual health insurance, but with a rider excluding coverage for a medical condition.
- Diagnosis of one of the medical conditions established by the Pool Board for automatic eligibility.
- Certification from an insurance agent that the applicant would be declined for substantially similar individual coverage by an insurer, due to health reasons.

HEALTH PLAN DISTRIBUTION in 2013 The Pool offered five deductible plan options.

Year-End Enrollment by Deductible Plan



Year-End 2013 Enrollment Eligibility Categories



NET LOSS The Pool's audited net loss for 2013 was \$141,797,651.

PREMIUMS EARNED & COLLECTED In 2013, the Pool collected \$158,921,621 in premiums from members, while total earned premiums for the year were \$192,078,425, including amounts paid by subsidies.

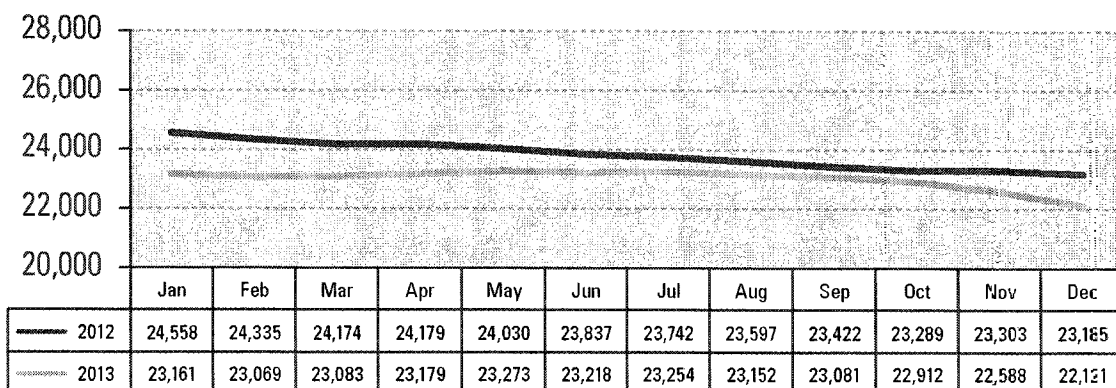
CLAIMS PAID & INCURRED Claims paid by the Pool during 2013 totaled \$322,295,044. Claim reserves decreased by \$3,720,000. A total of 565,643 medical claims and 769,841 prescription drug claims were processed.

ASSESSMENTS In 2013, the Pool assessed \$45.5 million to ±160 health insurers and HMOs.

ADMINISTRATIVE EXPENSES Third-party administrator fees in 2013 totaled \$12,159,119. All other operating expenses, including consulting, legal, actuarial, and agent fees, totaled \$1,190,716.

ENROLLMENT: In 2013, the Pool experienced a 2.9% decrease in enrollment, ending the year with a total of 22,121 members. The Pool covered 27,170 individuals over the course of the year. Members enrolled in the Pool at year-end had been covered for an average of 59 months. Pool members reside in every metropolitan area of the state and in all but 7 Texas counties (see p. 4 for county map). At year-end, 53% of the Pool's members were women. The average member age was 51 years; 70% of the Pool's members were in the 50-64 age group.

Enrollment by Month, Calendar Years 2012-2013



TEXAS HEALTH INSURANCE POOL
2013 FINANCIAL RESULTS (STATUTORY)

ASSETS, LIABILITIES, AND SURPLUS

2013

2012

ASSETS		
Cash and Short-Term Investments	\$56,646,341	\$88,571,308
Premiums Due and Unpaid	518,311	203,797
Third Party Administrator - Collected Premiums	64,171	740,617
Assessments Receivable	43,022,502	80,995,563
Furniture and Equipment, Net of Depreciation	3,397	6,885
Other Assets	0	1,700
Total Assets	\$100,254,722	\$170,519,870
LIABILITIES AND SURPLUS		
LIABILITIES		
Accounts Payable	\$1,067,334	\$1,199,105
Assessment Refunds	6,854,388	3,276,724
Unearned Premiums	2,107,661	8,300,705
Premium Discount Funds HB 2064	42,723,145	10,654,682
Y10/11 Fed Grant/Premium Trend	0	3,400,000
Reserve for Losses	32,730,000	36,450,000
Advance-Interim Assessment	156,575,097	226,190,760
Total Liabilities	\$242,057,625	\$289,471,976
SURPLUS		
Accumulated Regular Assessments Paid In	\$1,008,586,034	\$889,639,150
Cumulative Surplus (Deficit)	(1,150,383,684)	(1,008,591,256)
Net Surplus (Deficit)	\$(141,802,903)	\$(118,952,106)
Total Liabilities and Surplus	\$100,254,722	\$170,519,870

REVENUES AND EXPENSES

2013

2012

REVENUES		
Premiums - Paid by Policyholders	\$171,665,667	\$186,534,249
Premiums - HB 2064 Low Income Subsidies	12,139,185	12,034,998
Federal Grant - Premium Trend Subsidies	8,273,571	1,893,674
Federal Grant - Operating Losses	1,755,045	4,289,281
Net Investment Income	14,760	8,260
Total Revenues	\$193,848,228	\$204,760,462
EXPENSES		
Claims Paid and Incurred	\$322,296,044	\$310,612,516
TPA Administrative Fees	12,159,119	12,048,356
Professional Fees	424,447	360,332
Payroll and Employee Benefits	426,573	377,048
Agent Referral Fees	166,050	176,300
Office Rent and Insurance	77,148	70,654
Postage/Printing/Supplies	50,095	33,640
Bank Fees/Charges	13,286	365
Travel Expenses	2,785	3,129
All Other Expenses	30,332	25,005
Total Expenses	\$335,645,879	\$323,707,345
Net Loss	\$(141,797,651)	\$(118,946,883)



OFFICE OF THE GOVERNOR

RICK PERRY
GOVERNOR

September 17, 2013

Ms. Julia Rathgeber
Commissioner
Texas Department of Insurance
P.O. Box 149104
Austin, Texas 78714

Dear Commissioner Rathgeber:

During the 83rd regular session, the Texas Legislature passed and I signed into law Senate Bill 1795, which authorized the creation of rules regulating a navigator program to assist Texans in signing up for the federal health care exchange, which is a requirement under the Patient Protection and Affordable Care Act, otherwise known as Obamacare.

SB 1795 allows TDI to create and enforce regulations governing those persons who seek to work as navigators and specifically allows TDI to adopt more stringent regulations than federal rules. SB 1795 also prohibits navigators in Texas from engaging in electioneering activities.

The U.S. Department of Health and Human Services has repeatedly delayed explaining how its navigators were going to be created, how they were going to operate, and how they were going to be regulated.

Because of the nature of navigators' work and because they will be collecting confidential information, including birth dates, social security numbers and financial information, it is imperative that Texas train navigators on the collection and security of such data.

To that end, I am directing TDI to use its authority under S.B. 1795 and create rules to ensure that navigators are well-trained, qualified, and capable of protecting Texans' privacy.

Therefore, as TDI develops rules for regulating navigators, please ensure your rules require that navigators:

- Be at least 18 years old and demonstrate knowledge and capability to perform the services of a navigator;
- Provide proof of U.S. citizenship or legal residency;
- Complete a comprehensive, TDI-approved training course of a minimum of 40 hours coursework in addition to any federal coursework;
- Pass a rigorous exam based on that training course and covering job functions and privacy protections, among other topics;

Ms. Julia Rathgeber
September 17, 2013
Page 2

- Refrain from selling, soliciting, or negotiating health insurance, and from recommending a plan, providing advice regarding substantive benefits or comparative benefits of different plans;
- Submit to initial and periodic background and regulatory checks;
- Report to TDI on a regular basis the names of those persons they sign up for the federal health care exchange, and locations at which sign-ups take place.
- Show state issued identification and credentialing when approaching individuals, in advance of entering their home, or when otherwise intruding on their privacy.

Furthermore, TDI rules for the navigator program should:

- Create and require continuing education requirements;
- Require TDI to maintain a comprehensive database of navigators and their relevant information which includes background checks, regulatory checks and fingerprints;
- Include in TDI's database information on names of persons who were signed up in the federal health exchange by navigators and the locations at which they were signed up;
- Institute time, place, and manner requirements for navigator activity, including limiting registration of persons only between the hours of 8am and 8pm;
- Allow TDI to charge a fee sufficient to cover the costs of licensing, education, administration, and all other activities associated with the navigator program;
- Institute a surety bond for repayment to the state for any navigator's failure to secure confidential information, failure to maintain necessary training and certification, and improperly including ineligible individuals in the program;
- Give TDI the authority to suspend, or have registration revoked, for non-compliance or failure to meet any of the requirements created in rule or statute; and
- Give TDI the authority to take enforcement action against any person or entity that is holding itself out as, or performing the duties of, a navigator without being registered.

In addition to these, I trust that you will look at all of the ideas before you and give serious consideration to any additional proposals that seek to protect Texans and their privacy.

I look forward to working with you as we move through the rulemaking process.

Sincerely,



Rick Perry
Governor

RP:msk

Comparison of Key Provisions in the Proposed and Adopted Navigator Rule

Topic	Adopted Section	Proposed	Adopted
Registration and renewal application fee	N/A	\$50	\$0
Prohibitions	19.4013(a)(5) and (b)	Included prohibition on advising on the substantive and comparative benefits of health plans	Modified text to more closely reflect the language in the authorizing legislation. This language can be found in Section 4154.101(a)(4) of the Texas Insurance Code. Also, added (b) to reflect the provision of 4154.101(b)
Preregistration training requirements	19.4008(a)(2)	Included completion of 40 hours of state-specific training broken down into Medicaid (13 hours), privacy (13 hours), and ethics (14 hours).	Included completion of 20 hours of state-specific training broken down into Medicaid and CHIP (5 hours), privacy (5 hours), ethics (5 hours), basic insurance terminology and how insurance works (2 hours), preparation for the examination (2 hours), and the examination (1 hour)
Applicability date for registration	19.4003(a)	1-Mar-14	1-Mar-14
Applicability date for education and examination requirements	19.4008(g)	1-May-14	1-May-14
Surety bond requirement	19.4010(a)(1)	\$50,000 surety bond amount	\$25,000 surety bond amount
Providing information regarding health insurance and how the ACA works	19.4004	Registration not required to provide this service.	Registration not required to provide this service
Assisting friends and family	19.4003(f)	Not addressed	Exception included for individuals providing services to persons related within the third degree of consanguinity or within the second degree of affinity
Human resource (HR) personnel using SHOP	19.4003(e)	Not addressed	An exception is included for HR personnel using SHOP to provide qualified health plans to employees of the business
Use of the term "navigator"	19.4014	Prohibited those subject to the rule from using the term "navigator" unless registered with TDI	Clarified who is a "navigator" for purposes of this rule.

--	--	--	--

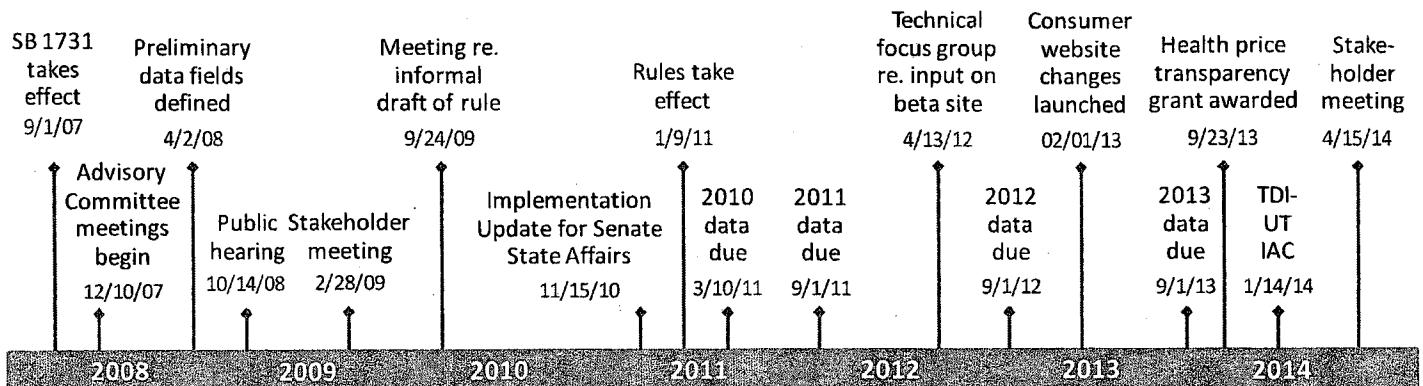
APPENDIX TO CHARGE 7

TDI'S EFFORTS TO PROMOTE TRANSPARENCY IN HEALTH CARE

STATUTORY TRANSPARENCY REQUIREMENTS

- In 2007, the 80th Texas Legislature passed SB 1731, which promoted transparency through a variety of approaches:
 - ◆ Requiring health plans to provide enrollees with cost estimates, upon request, in advance of a procedure
 - ◆ Requiring providers to provide uninsured and out-of-network patients, with charge estimates upon request
 - ◆ Creating TDI's Consumer Reimbursement Rate Guide, which provides average regional health care prices for certain health care services, based on claims data submitted by health insurers
 - ◆ Establishing an annual report card for health insurance companies that allows consumers to make direct comparisons of insurers' health plan benefits, costs, and quality
 - Implementation was temporarily suspended in order to avoid duplication with federal health reform requirements, which include some transparency reporting requirements for health insurers

PROGRESS TO DATE



- A partnership with UT on a federal grant has provided an opportunity to revisit TDI's health price transparency effort, evaluate progress to date, and make improvements to the Consumer Reimbursement Rate Guide
- TDI is also working to implement health insurer report cards, largely relying on data insurers are already producing to comply with other state and federal requirements

WHAT IS TDI'S CONSUMER REIMBURSEMENT RATE GUIDE?

- TDI's Consumer Reimbursement Rate Guide is an online tool that allows Texans to search for the average price for medical procedures in 11 regions statewide.
 - ◆ The tool relies on data that TDI has collected since 2010, pursuant to TIC §38.355 and TAC §§21.4501-4507.
 - ◆ The existing tool is of limited use to consumers due to inherent limitations in the data call design, data quality issues, and the format for presenting data.
- UTSPH will analyze technical issues with TDI's data collection process and make recommendations for improvement.
 - ◆ Issue: data in its current form does not allow TDI to report on the amount of variation in prices
 - ◆ Issue: data is missing some necessary fields, such as "units of service"
 - ◆ Issue: method for collecting data on inpatient and outpatient facility prices is overly simplified and does not account for the complexity involved in billing for services delivered in inpatient and outpatient facilities
 - ◆ Best practice: present prices on treatment event, rather than individual billing codes
 - ◆ Best practice: prioritize treatment events that are common, but also "shoppable"
- TDI hosted a stakeholder forum April 15, 2014, to collect additional insight from consumers and industry on how to transform the Consumer Reimbursement Rate Guide into a useful tool for Texans.

Abstract

HEALTH PRICE TRANSPARENCY GRANT

BACKGROUND

The objectives proposed under this grant represent a continuation of previous efforts by Texas policymakers to promote a consumer-driven health care system and empower consumers with the information they need to make better health care decisions. Legislative efforts have given Texas consumers the right to request estimates from providers and health plans on prospective charges and negotiated prices before scheduling a procedure. Consumers can find the average prices negotiated by insurers within a region for 439 specific medical procedure codes on the Consumer Reimbursement Rate Guide established by the Texas Department of Insurance.

Despite these strides, the complexity of health care pricing necessitates additional work to make price data more meaningful to consumers. Medical procedure codes make sense to medical billing specialists, but are less clear to the average consumer, who cannot predict all of the components a provider may include on a bill for a given procedure. Through the work of the Texas Institute for Health Care Quality and Efficiency, the challenges associated with price transparency have been discussed at length. Institute recommendations reflect the need to provide consumers with more timely cost estimates, encourage health plans to provide enrollees with transparency tools, and endorse the pursuit of voluntary participation by health insurers in a comprehensive claims database.

PROPOSED INITIATIVE

TDI was awarded a federal grant to support and enhance existing state efforts to provide transparent information on the price of health care services through the Consumer Reimbursement Rate Guide. TDI is pursuing activities under this grant in partnership with the University of Texas School of Public Health. This partnership will leverage UT's infrastructure, resources, and expertise to achieve the goals and objectives outlined below.

In addition to building on TDI's reimbursement rate data, this effort will utilize a database developed by the UT SPH, which contains comprehensive claims data from Blue Cross Blue Shield of Texas, Texas Medicaid, and Medicare. The level of detail in this dataset will inform TDI efforts to present pricing information in a format that is more reflective of a typical consumer experience. As additional private payers consider participating in this database, it provides a starting point for the research community to evaluate questions on a market-wide level.

GOALS AND OBJECTIVES

Activities pursued under this grant will seek to enhance efficiency in the use of Texans' health care resources by increasing health care price transparency and developing research to support best practices among insurers and providers. Primary approaches to achieving objectives include:

- Connecting consumers to meaningful information on health care prices and decision tools that support high-value treatment options
 - Grouping medical procedure codes to illustrate the full treatment event the average consumer may face for a given procedure, including average prices for each component and the episode as a whole
 - Identifying medical procedure codes associated with accepted treatment guidelines and connecting consumers to information on best practices for the treatment of certain conditions
 - Analyzing pricing variation across geographic regions and service settings to identify trends and synthesize useful tips for consumers (e.g., this procedure is less costly when performed in a doctor's office)
 - Improving the Consumer Reimbursement Rate Guide website to increase consumer understanding of the data
 - Supporting voluntary insurer efforts to provide meaningful, contract-specific price information to enrollees in real time through an insurer-hosted web tool
- Developing a comprehensive claims database to support research opportunities related to health care practices, payment methodologies, and health care utilization in Texas, managed by the UT School of Public Health in partnership with the Texas Department of Insurance
 - Creating a cooperative environment among commercial carriers to share data for research without forfeiting the confidential status of proprietary data
 - Providing research opportunities in health economics, health policy, and health utilization management
 - Sharing analysis and findings with Texas leadership to inform policy decisions
 - Enhancing TDI's ability to act as a resource for leadership on issues related to health care cost and utilization

APPENDIX TO CHARGE 8

APPENDIX TO CHARGE 10

**History of the Workers' Compensation
Insurer of Last Resort
(Residual Market)
September 2014**

History of Workers' Compensation Residual Market

- **1953** – Texas Workers' Compensation Assigned Risk Pool (TWCARP) was created by the legislature effective October 1, 1953.
- **1987-1991** – TWCARP was the largest writer of workers' compensation insurance in the state. Many insurance companies were restricting their writing of workers' compensation insurance in Texas in an attempt to lower their assessments to pay the ever-increasing deficits of the TWCARP.
- **1991** – Name of residual market changed by legislature to Texas Workers' Compensation Insurance Facility (TWCIF).
- **1991** – Legislature created the Small Premium Policy Plan (SPPP) requiring insurance companies to write workers' compensation policies with premium less than \$5,000 in their voluntary book of business as a means to de-populate the TWCIF.
- **1993** - December 31, 1993, was the effective date of the last policies written through the TWCIF.
- **1994** – Insurer of last resort was created by legislature as part of the Texas Workers' Compensation Insurance Fund (Fund).
- **1994** – January 1, 1994, was the effective date of the first policy written through the insurer of last resort (START program) at the Fund.
- **2001** – Name of the Fund was changed to Texas Mutual Insurance Company (TMIC) effective September 1, 2001, and continued to also be the insurer of last resort.

Basics of Law Pertaining to Workers' Compensation Insurance

- Rates are File and Use (TIC, Chapter 2053).
- The residual market is written by TMIC through the START program (TIC Chapter 2054, Subchapter H).
- Purpose of TMIC (TIC Section 2054)
 - serve as a competitive force in the marketplace
 - guarantee availability of workers' compensation insurance, and
 - serve as the insurer of last resort.
- Rates for TMIC, including the insurer of last resort, must be sufficient, when invested to (TIC chapter 2054, Subchapter F)
 - carry all claims to maturity
 - meet reasonable expenses of conducting the company's business, and
 - maintain a reasonable surplus.
- Rates filed for the START program are +50.00% above the relativity.
- The START program filed schedule rating plan provides for a maximum credit and a maximum debit of $\pm 75\%$.

Key Statistics for Texas Mutual Insurance Company and the Residual Market for Calendar Year 2013

	Number of Policies	Direct Written Premium	Percentage of Direct Written Premium to Total Market Premium
Texas Mutual - Voluntary Business	62,771*	\$1,025,928,467	38.8%
Texas Mutual - Residual Market	122	\$5,428,211	0.2%
Texas Mutual - Total	62,283	\$1,031,356,678	39.0%
Total Workers' Compensation Market	204,520	\$2,644,942,617	100.0%

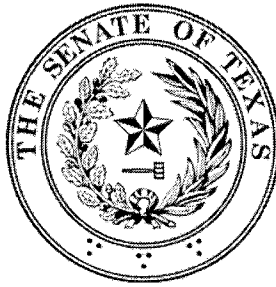
*Texas Mutual Insurance Company was the source for the number of policies written in their voluntary business. (Source for all other numbers in this table is the Quarterly Legislative Report on Market Conditions, 4th Quarter 2013.)

History of number of policies written and premium volume for the workers' compensation residual market based on historical data at the Texas Department of Insurance for years 1969-1993 and as reported on the Quarterly Legislative Report on Market Conditions Report from 1995-2013:

Year	Number of Policies Written	Premium Volume
1969	4,515	\$5,742,859
1989	85,758	\$850,116,288
1991*	31,972	\$1,284,799,469
1993	10,744	\$303,113,619
1995	2,195	\$27,435,325
2000	545	\$17,063,620
2002	579	\$32,949,993
2005	186	\$9,815,378
2010	91	\$2,866,651
2011	90	\$2,308,019
2012	112	\$3,928,161
2013	122	\$5,932,463

* The Small Premium Policy Plan was enacted in 1991, requiring insurance carriers to write workers' compensation policies with premium \$5,000 and below as part of the carrier's voluntary book of business in an effort to depopulate the Texas Workers' Compensation Insurance Facility.

- 1953 through 1990 – Texas Workers' Compensation Assigned Risk Pool
- 1991 through 1993 – Texas Workers' Compensation Insurance Facility
- 1994 through August 31, 2001- Texas Workers' Compensation Insurance Fund
- September 1, 2001 through present – Texas Mutual Insurance Company



January 22, 2015

The Honorable Craig Estes
Chair, State Affairs Committee
Texas Senate
Room 3E.18
Austin, Texas 78701

Dear Chair Estes:

Thank you for your leadership and your work on the Committee's joint report to the 84rd Legislature. We are honored to serve with you as we work to address issues vital to the future of our state. We know that the joint report reflects months of hard work by the Committee, however we would respectfully like to add a few additional points regarding the Federal Affordable Care Act (ACA) and to encourage continued policy discussions that weigh both the costs and benefits of key provisions of the law.

The State will face a number of challenges and issues related to the ACA, but what the Legislature decides to do going forward may well determine the future of health care in our state and whether or not the uninsured and under-insured have real access to affordable care. Texas leads the nation in percentage of uninsured and stands to benefit greatly from the implementation of the ACA.

While the Committee was tasked with studying the emerging negative impacts of the ACA, it is important to note that many people are benefiting from the law. Those who were able to enroll now have access to comprehensive coverage as health plans are required to offer ten essential benefits, including emergency care, prescription drug benefits, and preventative care. In addition, young adults are able to stay on their parents' insurance plans, including those previously in foster care who are now eligible for Medicaid until 26 years of age.

Uninsured rates nationally and in Texas are declining, and according to estimates fifty-seven percent of marketplace enrollees nationally were previously uninsured. In Texas, enrollment surpassed what was originally projected with nearly 734,000 Texans selecting a plan during the first open enrollment period. Eighty-four percent of those who enrolled in Texas received financial assistance.


The report mentions that the estimated 734,000 enrollees only represent twenty-three percent of the potential enrollees in Texas, but it is also important to note that the State has not been an active partner in helping inform and enroll Texans in these new coverage options. As a result, navigators are and will remain a critical resource for enrollment assistance, especially for vulnerable and underserved populations. They are trusted sources of information in their communities and are able to use these

connections to inform consumers about health insurance and financial assistance options available through the marketplace. Many of these organizations have a long history of helping people enroll in Medicaid, CHIP, and Medicare.


Lastly, the report details the issue of increasing premiums. Preliminary analyses of 2015 rates show that some marketplace premiums are going down and others are increasing, but in general most increases are modest and lower than pre-ACA rates. In addition, a recent survey by Kaiser Family Foundation found that the annual rate of increase in employer premiums is at the lowest rate since Kaiser started conducting the survey 16 years ago. The average premium cost of family coverage grew by only three percent from 2013 to 2014.

We thank you in advance for considering our comments, and we look forward to working together during the 84th Legislative Session.

Sincerely,



Senator Rodney Ellis



Senator Eddie Lucio, Jr.



