Circuits

Newsletter of the
Computer and Technology Section – State Bar of Texas
May 2018

Contents

Message from the Chair

By Michael Curran

Greetings from the Computer and Technology Section! We greatly appreciate our community of members and look forward to serving all Texas attorneys throughout the year. It is our Section's mission to be a resource to the legal profession in matters involving technology. To that end, we have focused on providing new legal tech educational opportunities to lawyers during the past year.

First, our Section sponsored the ***With Justice and Technology for All*** CLE, a course focused on providing pro bono and new lawyers with recommendations on using technology to enhance their practice. We would like to thank Chief Justice Hecht for his keynote address and the many outstanding speakers who made this event a success.

We continue to offer ***Circuits***, our members-only newsletter. We added several free educational videos to ***Tech Bytes***, which are available to all Texas lawyers at texasbar.com/tech-resources. Typical topics addressed include encryption, privacy, data breaches, and eDiscovery. Section members also continue to enjoy complimentary use of our **Texas Bar Legal App**, which gives you access to current Texas rules and codes with links to relevant case law.

The final live event for our Section this year is the **Adaptable Lawyer** track held during the State Bar of Texas Annual Meeting in Houston on June 21-22. Our Section is co-sponsoring the Adaptable Lawyer CLE track, which includes two days of legal technology topics. There will also be a Section general membership meeting following one of the CLE talks and a happy hour in the evening of June 21.

If you wish to learn more or get involved with the Computer and Technology Section, please contact our Section administrator at admin@sbot.org.

Thank you again for your membership and your interest in matters related to technology and the law.

Michael Curran, 2017-2018 Chair of the Computer and Technology Section, State Bar of Texas

COMPUTER AND TECHNOLOGY SECTION

Letter from the Editor

By Kristen Knauf

It feels a bit unnatural to reflect on the end of the year just as the weather is starting to turn warmer. Is this what it feels like to celebrate New Year's Eve in the southern hemisphere? In any event, this last issue of *Circuits* for the 2017–2018 bar year covers several hot technology topics.

First, Hannah Allison and Briana Stone share some heartwarming stories about using technology to close the justice gap in Texas. It only takes twenty minutes to register at TexasLegalAnswers.org and answer a legal question posed by a fellow Texan in need. I, myself, have answered a handful of these questions, and would encourage my fellow Section members to participate in this easy, innovative *pro bono* service opportunity.

Next Craig Ball examines Federal Rule of Civil Procedure Rule 37(e) to determine whether a failure to preserve electronically stored evidence could be used to prove bad intentions.

Now that all fifty states have passed data breach notification laws, will state legislatures turn their attentions to data privacy laws? John G. Browning takes a closer look at the strict biometric data privacy laws in Illinois, Texas, and Washington.

Continuing the focus on data privacy, Pierre Grosdidier discusses the Children's Online Privacy Protection Act (COPPA), and analyzes recent case law and FTC enforcement actions. COPPA: It's not just a plot point on the HBO show *Silicon Valley*.

Finally, Elizabeth Rogers and Aaron Gregg have prepared an update on Texas Cybersecurity laws. Given the many changes in this area of law, their update will be published in two parts. Part 1 is featured in this issue, while Part 2 will be in our Fall 2018 issue. Be sure to renew your Section membership so that you do not miss the next issue of *Circuits*!

We hope that you enjoy reading *Circuits*, and welcome any comments that you may have: send them to our section administrator at admin@sbot.org. Many thanks to Antony P. Ng, Elizabeth Rogers, and Michael Curran for their assistance with *Circuits* this year. It has been a privilege and a pleasure to serve as editor to this publication, and I hope to see you at the upcoming State Bar of Texas Annual Meeting (June 21–22) in Houston.

Warm Regards,

Kristen Knauf

Closing the Gap in Texas, One Question at a Time

By Hannah Allison & Briana Stone

Outside of Arlington, Judith Rojas heard the alert on her phone: "A volunteer attorney has responded to your question." She had been feeling increasingly helpless in her attempts to get her landlord to repair her heater. As the temperature dropped, she was forced to leave the stove open at night for heat, which she knew was dangerous. Worried about her safety, Judith's brother told her about a new, free online legal advice clinic called www.TexasLegalAnswers.org where she would be able to communicate with an actual attorney. Sighing with relief, Judith read the attorney's encouraging, step-by-step advice and felt empowered and hopeful for the first time in months.

Meanwhile in Fort Worth, Angela Wilson logged off Texas Legal Answers just as her son climbed into her car, already excitedly recounting the day's adventures. While waiting in the elementary school pick-up line, she had answered a question from a young mother, not so unlike her, who was having trouble with her landlord. She had told the woman what she needed to know to get her landlord to fix her heater, hopefully before the next major cold front. Although she sometimes felt overwhelmed balancing her busy work and family life, making time to give back was important to her and Texas Legal Answers made it easy. Since reading about it on Facebook, she had already answered several questions, each time spending about 20 minutes from start to finish. She loved that she could squeeze it in whenever she had a couple minutes and that she could choose which questions she wanted to answer, but the real reason she kept going back was that it always lifted her spirits.

Together these two stories illustrate the exciting mission of the Texas State Bar's newest pro bono initiative—to help close the justice gap one question at a time. This past June, the State Bar's Legal Access Division launched TexasLegalAnswers.org, a free, online legal advice clinic where Texans trying to make ends meet can post their civil legal questions and get answers from volunteer attorneys. The format ensures that rural Texans and others who lack access to traditional legal aid can get help, and it provides a flexible volunteer opportunity for lawyers across the state. So far, users have posted more than 2,500 civil legal questions and over 240 Texas attorneys have signed up to volunteer. A new volunteer recently said, "I like to think that

by answering these questions, I am helping those who have had to make the choice between purchasing groceries or paying attorney fees."

Texas Legal Answers has also developed exciting partnerships with law schools across the state. Under the supervision of faculty, law students at St. Mary's School of Law and University of Houston Law Center have answered questions posted on the TexasLegalAnswer.org website as part of their class assignments intended to give law students hands-on experience researching and answering real legal questions in plain language. Meanwhile, Baylor Law School hosted a Texas Legal Answers clinic at a local law firm where students worked in groups with practicing attorneys to answer questions. The clinic was so successful that Baylor Law School is planning to make it an ongoing event. Similarly, South Texas College of Law Houston is incorporating Texas Legal Answers into its clinical program to provide additional pro bono opportunities for its law students as well as the chance to work closely with faculty.

After receiving many positive responses from the legal community and the public in the first six months since the inception of the program, the focus for Texas Legal Answers will now be on recruiting more volunteer attorneys and building partnerships with law firms, corporate legal departments, bar associations, and any groups who are interested in an easy and innovative pro bono opportunity. If you are ready to **#Give20Minutes** to help your neighbor, visit www.TexasLegalAnswers.org and click on 'Volunteer Attorney Registration' to get started. If you would like to learn more about hosting a Texas Legal Answers clinic or to schedule an MCLE-accredited presentation about Texas Legal Answers for your members and/or employees, please contact LegalAnswers@TexasBar.com.

Inquiring into Intent: FRCP Rule 37(e) Opens the Door

By Craig Ball

Lawyers spend a ton of time thinking about intent. Intent is what separates murder from negligent homicide. It's key to deciding whether minds have met to form a binding contract. Intentional torts are punished differently from negligence. Notions of intent pervade the law: testamentary intent, transferred intent, malice, bad faith, *mens rea*, scienter and premeditation. The intent of the framers of the U.S. Constitution was the linchpin of the late Justice Antonin Scalia's interpretation of that great document.

Intent is the attitude with which one acts. It can be general intent in the sense of acting in the way you meant to act, or it can be specific intent in anticipating and seeking a specific outcome. *Intent is all in the mind*.

Proving intent is one of the harder things trial lawyers do. Short of the rare Perry Mason moment when a party confesses intent (*i.e., "You're damn right I killed him, and I'd do it again. The bastard NEEDED killing!!"*), lawyers must resort to evidence that illuminates the intent of a specific person or corporation or that of a reasonable person or corporation similarly situated in terms of what he, she or it would have thought, anticipated or known.

When lawmakers demand proof of intent, they necessarily contemplate that evidence of intent be brought forward. Lawyers must be able to delve into intent and discover direct and circumstantial evidence of intent. We must be permitted to probe the knowledge, experience, attitudes, motives, expectations and prejudices of the person or entity whose intent is at issue.

Because intent is elemental but difficult to prove directly, the law gives leeway to the discovery process. For example, Courts generally prohibit evidence of other wrong acts or bad character to prove a specific act in accordance with character or traits but make an exception and permit the evidence to come in when prior bad acts show intent (Federal Rules of Evidence § 404(b)(2)).

All of this is prelude to discussing the broader impact of amended Rule 37(e) of the Federal Rules of Civil Procedure (FRCP), now requiring a finding of an "intent to deprive" as predicate for sanctioning evidence destruction and discovery obstruction. As I hope all my readers know, FRCP Rule 37(e) was amended effective 2015 to state:

(e) **Failure to Preserve Electronically Stored Information.** If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:

(A) presume that the lost information was unfavorable to the party;

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment.

The wording of the amended rule sprung from political compromise. I assuage the wailing and gnashing of teeth for those who hate the rule by reminding them what a maggot-ridden pile of excrement it would have been had not cooler heads prevailed. Will it serve to shield those who care nothing for competency in e-discovery? Yes, it's already served that purpose in reported cases; *see*, *e.g.*, *OrchestrateHR, Inc. v. Trombetta*, 178 F. Supp. 3d 476 (ND Texas 2016). But, unless the amended Rule was intended to immunize bad actors—and I'm certain that was not the goal of most who worked on it—requiring proof of intent to deprive also brings discovery of evidence going to intent within scope when spoliation of ESI is an issue.

Though "intent to deprive" has been an element of criminal theft for ages, there isn't much discovery in criminal matters, so little precedent to draw on. I suspect those drafting the rule gave little thought to how adding the element of intent would necessitate fulsome discovery into intent. But, if the justice system is to operate fairly, parties must be permitted to collect evidence concerning the requisite elements of proof. Anything less is a rigged system.

What does this mean for discovery? To start, it suggests that questions of the sort that might have been out-of-bounds before are now relevant and material lines of inquiry. If the "intent to deprive" of a party is at issue, then questioning the party and its representatives concerning knowledge, experience, attitudes, motives, expectations and prejudices of the actors must be pursued and permitted. Getting to bad faith and evil intent is an ugly business. It requires scrutiny of our meanest, basest aspects of our character. But, if you are going to make movants prove scienter, then you must let movants marshal the evidence of same. Inquiring

into motive, attitudes and expectations is not fishing; it is looking in the dark places where intent hides.

I also suspect that the drafters of the amended rule did not ponder how the obligation to prove intent to deprive would collide with claims of privilege.

Lawyers are nuts about privilege, and I mean that in every sense of the word. They love to claim that anything having anything to do with pending or anticipated litigation is work product, and most lawyers are irrationally exuberant when it comes to client communications pertaining to matters in litigation.

So, ask yourself, "in what context are communications and information about efforts to deprive opponents of information most likely to occur?"

Clearly, intentional efforts to deprive parties of evidence will find most frequent expression in contemplation of litigation and in communications about what the lawyers have instructed clients to do in terms of preserving and producing information in discovery. So, how do we balance sweeping claims of privilege against the right to discover intentional destruction of evidence?

To start, courts must address where the crime/fraud privilege exception fits with respect to whether evidence of intentional spoliation can be discovered. I sympathize with those who charge that the assertion of privilege in litigation has gone off the rails, to the point that privilege is a velvet rope to keep the public from incriminating information. Lawyers have become so cavalier in their assertion of privilege that it makes a mockery of the noble and essential principles behind the privileges. How will movants explore the intent of in-house counsel? What is the role of neutrals in such inquiries? It's a swamp, and the amended rule requires we wade in.

Lawyers must frame new lines of inquiry for deposition and discovery going to proof of intent when data is lost. Will lawyers be questioning IT staff about how they feel about the requesting party? About people who sue? Do we plumb the attitudes about and between counsel? When the issue is intent, questions about attitudes, biases, experience, expectations, background and emotions figure into the inquiry.

Rule 37(e) has closed some doors, but it has also opened others. When Rule 37(e) applies, the right of a deprived party to discover evidence bearing on intent to deprive seems manifestly

clear to me; but, it is also clear that the assertion of this right will be fought tooth and nail by spoliators who want the benefit of Rule 37(e) without bearing the burden.

Such is the nature of unintended consequences. Those who fought for protection from the consequences of their misconduct failed to consider that they were putting their conduct under a new microscope. It will be up to judges to find the appropriate balance between the rights of the spoliator and the rights of those prejudiced by spoliation.

Let's hope that, in wisely seeking not to punish the merely negligent, courts still seize on the opportunities to deter ignorance, incompetence and complacency that unintentionally-but-prejudicially deprives litigants of relevant evidence. There are no carrots luring us to e-discovery competence; all the courts have are sticks.

The Battle Over Biometrics

By John G. Browning

In January, as Google debuted the "art selfie" feature on its Google Arts & Culture app—enabling people to find their art lookalikes from over 1,200 museums worldwide—users delighted in the chance to match themselves to a painting or sculpture. All Google users, that is, except those in Illinois and Texas. In those two states, the app was blocked for fear of violating the strict biometrics privacy laws on the books there. But just what do such statutes cover, and as biometrics measures became more commonly used by everyone from banks and credit card companies to employers, will laws like those in Texas and Illinois pave the way for similar privacy legislation?

First, it is important to note that commercial use of biometrics data—measurements of one's physical being—has exploded in recent years. With advances in sensors, software, and readers, it has become simpler than ever to employ such things as fingerprints, facial recognition, retinal or iris scans, voiceprint reading, gait analysis, or even keystroke analysis to identify a person. With its accuracy and ease of use, biometric data is being used as part of the authentication protocol for physical devices (like smart phones), online applications, and telephone calls. Banks, for example, regularly employ voiceprint, using a digitized representation of the sound of a customer's voice to authenticate that account holder when he or she calls a customer service line. In February 2016, MasterCard announced that it would accept "selfies" as passwords, allowing cardholders to access their accounts using their faceprints.

But the use of biometrics for identification presents certain pitfalls as well. Unlike a password or Social Security number, a person's biometric data is unique and immutable, and therefore cannot be changed or replaced. Once compromised, a biometric identifier may be lost, leaving the affected individual at a heightened risk for identity theft. In addition, use of biometrics opens up a whole new level of government surveillance. The FBI is already working on "Next Generation Identification," a program that collects voiceprints, iris scans, and other biometric data to supplement its current fingerprint identification system. Facial recognition technology in particular has been used by law enforcement, the Department of Homeland Security, and the Department of Defense for years.

And with such advantages as well as risks, it only makes sense that the capture and use of biometric data would attract legislative scrutiny. Laws addressing biometrics fall into two

categories: laws that specifically involve the collection and use of such data by private actors (like businesses) and governmental entities, and broader privacy laws that happen to include biometric information in their definition of personal information. This article will focus on the first type of laws, and particularly on the three states—to date—that have adopted laws regulating the collection, storage, and use of biometric data: Illinois, Texas, and Washington.

Illinois

Illinois was the first state to address business' collection of biometric data with the Illinois Biometric Information Privacy Act (BIPA) in 2008.[1] BIPA sets forth a comprehensive set of rules for companies collecting biometric data, and significantly (unlike its Texas and Washington counterparts) it creates a private cause of action for Illinois residents whose biometric data is collected or used in violation of these rules. Essentially, there are five key features of BIPA:

(1) it requires informed consent prior to collection;
(2) it prohibits any profiting off biometric data;
(3) it allows only a limited right to disclose the data;
(4) it sets forth both protection obligations and data retention guidelines for businesses;
(5) it creates a private cause of action for those harmed by BIPA violations.

As to the first of the above-mentioned five features, BIPA mandates that a business must give an individual written notice of the collection of biometric data. This notice must specify the purpose of the collection as well as how long the data will be used or stored. In addition, it must receive the individual's written consent. The content and form of this release, however, are not specified. Are electronic notices and releases satisfactory? Probably so, particularly if the terms and conditions are set forth explicitly, along with an "Accept" or "I consent" button.

The second feature, prohibiting a company from selling or "otherwise profiting" from the biometric data it collects and/or stores, doesn't have much more to it then what the statute's somewhat vague language provides. The third feature, concerning disclosure, bars a business from disclosing a person's biometric data unless: (1) the person consents; or (2) the disclosure completes a financial transaction that the individual requested; or (3) the disclosure is required by applicable state, federal, or local law; or (4) the disclosure is required pursuant to a valid warrant or subpoena.

As to the fourth feature, BIPA requires a business to give biometric data the same degree of protection as other sensitive, confidential information in its possession, employing the

[1] 740 ILCS 14, *et seq.*

reasonable standard of care within its given industry. The business may not store such data for more than three years from when the initial purpose of collecting the data was fulfilled, or three years from the affected individual's last interaction with the company (whichever is earlier). In addition, the business must have a written, publicly available retention/destruction policy, and must adhere to this policy. Finally, the fifth feature provides a private cause of action to anyone harmed by a business' violation of BIPA. Per the statute, a prevailing party may recover either actual damages or statutory damages of $1,000 (whichever is greater) for each negligent violation, and $5,000 in statutory damages for each intentional violation (or actual damages, depending on which is greater).

BIPA received little fanfare in the immediate wake of its enactment, but a series of 2015 lawsuits against online platforms Facebook and Shutterfly over their collection storage, and use of biometric data, specifically faceprints/facial geometry, brought renewed attention to the law and its privacy implications.[2]

Texas

Texas' biometric privacy statute[3], enacted in 2009, might well be called "BIPA-lite." Like its Illinois counterpart, Texas' law applies to the same kinds of biometric information, although unlike BIPA, it does not cover data that is converted into a code or template. Texas' statute only protects biometric identifiers, and doesn't contain a broader "biometric information" provision. Both the Illinois and Texas laws require notice and consent, but unlike BIPA, Texas doesn't require a written release. Like BIPA, Texas' statute prohibits the sale of biometric information, and both have restrictions on how it is stored. Texas and Illinois both require employers to store, transmit, and protect the data using reasonable care and in the same manner as the business treats other confidential information. And although both Illinois and Texas require that businesses destroy biometric data that is no longer needed, Texas puts that duty on a faster timetable. Under Texas' statute, the company must destroy such data "within a 'reasonable time' that does not exceed one year after the biometric data is no longer needed."[4] Of course, the biggest divergence between the two laws is that Texas does not allow

---

[2] *See, e.g.*, Pezen v. Facebook, Inc., 1:15-cv-03484 (N.D. Ill. Apr. 21, 2015); Licata v. Facebook, Inc., 1:15-cv-04022 (N.D. Ill. May 5, 2015); Patel v. Facebook, Inc., 1:15-cv-04265 (N.D. Ill. May 14, 2015), Gullen v. Facebook, Inc., 1:15-cv-07861 (N.D. Ill. Aug. 31, 2015); Norberg v. Shutterfly, Inc., 1:15-cv-05351 (N.D. Ill. June 17, 2015).

[3] TEX. BUS. & COM. CODE ANN. § 503.001.

[4] *Id.* § 503.001(c)(3).

for a private cause of action. Under Texas' statute, the attorney general can sue to enforce the statute and seek up to $25,000 per violation.[5]

Washington

Washington's biometric privacy statute took effect July 23, 2017.[6] Like its counterparts, it covers biometric measurements, but it also defines biometric information more broadly—as any "data generated by automatic measurements of an individual's biological characteristics."[7] Like the Texas statute, the Washington statute does not specify that consent must be in writing, nor does it create a private cause of action against violators. Its notice and consent provisions, however, do contain an exception that the others don't, carving out an exemption for biometric data collected and stored by the business for "security purposes." This applies to biometric data being stored for "the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value."[8] And unlike in either Texas or Illinois, under certain limited circumstances or with consent, a business may sell biometric information.[9]

The battle over biometric data continues to rage. Other states have considered legislation similar in many respects to the three laws discussed here, including Alaska, Connecticut, Montana, New Hampshire, and Utah. And lawsuits—particularly class actions—continue to be brought under BIPA. But it is not just tech companies that find themselves in the crosshairs. Since July 2017, more than twenty-five cases have been filed in state and federal courts in Illinois against video game companies, food product manufacturers, gas stations, and even restaurant chains (Wow Bao was sued over its use of facial scans to verify customer orders at self-service kiosks). And with employers using timekeeping systems and security protocols that use biometric identifiers (such as fingerprints or facial scans), the employer/employee relationship will continue to be a battleground for potential liability.

In short, facial recognition technology and other biometric measures will continue to be applied, even if the residents of Texas and Illinois do not get to enjoy the occasional innovation like Google's "art selfie." But businesses and their lawyers will have to navigate an increasingly complex regulatory environment in order to ensure compliance.

---

5 *Id.* § 503.001(d).

6 WASH. REV. CODE ANN. § 19.375, *et seq.*

7 *Id.*

8 *Id.*

9 *Id.* at § 19.375.020(3).

Mind the COPPA Rule protecting children online or expect to hear from the FTC

By Pierre Grosdidier – Haynes and Boone, LLP

If Internet-connected toys catch your attention and your kids' fancy, rest assured you are not alone. The Federal Trade Commission ("FTC") is watching them too, but not because its counsel are itching to buy them for their progeny. Instead, the FTC is focused on enforcing the toys' compliance with the Children's Online Privacy Protection Act ("COPPA," 15 U.S.C. §§ 6501–6506). COPPA and its regulatory embodiment, the COPPA Rule, aim to protect the online privacy of children under 13.[1] Congress tasked the FTC with the statute's enforcement.[2] A violation of the COPPA Rule "constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act."[3] The recent settlement between the FTC and VTech Electronics Ltd., a seller of Internet-connected toys, games and apps, shows that companies that sell online products to children must comply with the COPPA Rule or risk the travails attendant to a regulatory enforcement action.[4]

COPPA grants parents ultimate control over the collection and disposition of information that Web sites and online service providers ("operators") collect from children. The law applies not only to operators that target children, but also to operators that use others to collect information and to operators that have actual knowledge that information is collected from children.[5]

The law requires that qualifying operators seek "verifiable parental consent" prior to collecting, using, or disclosing children's personal information.[6] Such consent can be secured through means that "must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."[7] For example, a parent can be asked to provide a signed consent form or call an appropriately staffed toll-free call center. The list of verification methods is not exhaustive and parties can petition the FTC to approve new ones.[8]

---

[1] 16 C.F.R. § 312 ("Children's Online Privacy Protection Rule," prescribed in 15 U.S.C. 6502(b)).

[2] 15 U.S.C. § 6505(a).

[3] Complaint, *United States v. VTech Elecs. Ltd*, No. 1:18-CV-114, at 2, 10 (N.D. Ill., Jan. 8, 2018) (citing 15 U.S.C. § 6502(c); 15 U.S.C. § 45(a)) (Pacer Doc. 1).

[4] Order, *VTech*, No. 1:18-CV-114 (Pacer Doc. 2-1).

[5] *Id.* § 312.2 (*see* definition of "Operator").

[6] *Id.* § 312.5.

[7] *Id.*

[8] *Id.* § 312.12.

Recently, the FTC approved a verification method based on "knowledge-based authentication," a technique that uses questions that a child would struggle to answer. The FTC also approved a method that involves facial recognition software to compare two photos of the parent, one from the parent's government-issued identification (*e.g.*, driver's license or passport) and the other of the parent taken with his or her phone camera.[9]

The operator must make the collected information available for review by the parent, who can refuse to allow the operator to collect, use, or retain the information.[10] The operator must also prominently display on its home page and on the pages where children's information is collected a "clearly labeled link" to its information practices.[11] Other provisions apply to ensure the personal information's confidentiality, security, integrity, and eventual deletion.[12]

The law defines the term "personal information," as it applies to children, extremely broadly.[13] It includes not only the usual name, address, and phone and social security numbers, but also photos and video and audio files of children. Significantly, the definition also includes any information that can be used to track children through Internet, namely

> [a] persistent identifier that can be used to recognize a user over time and across different Web sites or online services[, including] . . . a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier; . . . [or] . . . Geolocation information sufficient to identify street name and name of a city or town.[14]

It is easy to imagine how Internet-connected toys in this Internet-of-Things ("IoT") era can create situations that run afoul of COPPA. A child's toy or stuffed animal with an Internet connection or an embedded GPS device might suffice if the child registered the toy on the manufacturer's Web site to activate the warranty or to download a matching app.

---

[9] FTC online Tips & Advice, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business (June 2017). The Web page contains the links to the FTC's approval letters.

[10] *Id.* § 312.6(a).

[11] *Id.* § 312.4(d).

[12] *Id.* § 312.8, 10.

[13] *Id.* § 312.2 (*see* definition of "Personal information").

[14] *Id.*

Recently the FTC settled its first-ever "children's privacy case involving Internet-connected toys."[15] In *United States v. VTech Elecs. Ltd.*, the government alleged, *inter alia*, that VTech sold "electronic learning products" or "ELPs" aimed at children younger than ten years old.[16] The complaint alleged that children could use the ELPs to access VTech-created online games, and also a VTech-developed online service called the Learning Lodge Navigator. Users could download from the Learning Lodge apps, games, e-books and other VTech-developed online material targeted at children. In the U.S. alone, parents had created Learning Lodge accounts for almost three million children by year-end 2015.[17] One of the downloadable ELP apps was Kid Connect, a children's communication app. By year-end 2015, the number of children with Kid Connect accounts approached 640,000.

The FTC complaint alleged that VTech violated COPPA by, *inter alia*:

- failing to obtain verifiable parental consent for collecting or using children's personal information;
- failing to post links to its children's information practices on its Web pages;
- "failing to provide direct notice to parents" of its children's information practices; and
- failing to implement and maintain a comprehensive information security program.[18]

Compounding VTech's predicament, and demonstrating the inadequacy of its information security measures, VTech learned from a journalist in late 2015 that it had been the victim of a data breach. The hacker penetrated VTech's test environment, then navigated into its live environment where it collected Kid Connect records containing children's personal information. The complaint alleged that the hacker penetrated VTech's network without authorization "by exploiting commonly known and reasonably foreseeable vulnerabilities." The hacker was even able to access a database that contained decryption keys for encrypted stored children's information, including photos and audio files.[19]

In a stipulated order resolving all issues addressed in the complaint, VTech was "permanently restrained and enjoined from violating" the COPPA Rule and was ordered to pay a $650,000

---

[15] Press Release, Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act (Jan. 8, 2018).

[16] This article discusses only the Internet-connected toys aspects of the FTC's complaint.

[17] *Vtech*, No. 1:18-CV-114, at 3–4.

[18] *Id.* at 10.

[19] *Id.* at 8–9.

judgment to the United States as a civil penalty.[20] Additionally, VTech was ordered to develop and implement a plan to comprehensively overhaul its information security practices. This plan must be audited by an independent third-party for 20 years.[21]

VTech follows in the footsteps of two other COPPA Rule-related complaints that the FTC settled in late 2015. Both complaints alleged—for the first time—that companies breached the COPPA Rule by allowing advertisers to use persistent identifiers to target children with advertisements. As noted, a persistent identifier is electronic personal information (*e.g.*, an I.P. address) that can be used to track a user over time and across Internet. The FTC added persistent identifiers to the definition of personal information in the COPPA Rule in 2013.

In *United States v. LAI Sys., LLC*, the complaint alleged that LAI offered children-targeted apps for download.[22] The apps consisted of games for, *inter alia*, virtual cooking and hair styling. The apps were free to download and LAI generated revenue through in-app advertising and purchases. LAI allowed third-party advertisers to collect underage users' persistent identifiers through the apps to better target their advertisements across Internet sites and over time.[23]

The complaint charged LAI with failure to give proper notice on its Web site of its information collection, use, and disclosure practices, failure to provide direct notice to parents of same, and failure to obtain verifiable parental consent before collecting or using children's information.[24] LAI was ordered to pay a $60,000 judgment and to henceforth abide by the COPPA Rule.[25]

Likewise, in *United States v. Retro Dreamer*, the complaint alleged that Retro Dreamer and its two executives sold or provided free of charge game apps for children. The apps generated revenue from their sale and through in-app advertising and purchases. The complaint's allegations against Retro Dreamer were essentially identical to as those against LAI. But in this case, the complaint further alleged that the defendants were aware of COPPA's existence and were told of the July 2013 rule change regarding persistent identifiers, but discounted the

---

[20] Order, *VTech*, No. 1:18-CV-114, at 8–9.
[21] *Id*. at 11–13.
[22] Complaint, No. 2:15-CV-9691, at 2, 10 (W.D. Cal., Dec. 17, 2015) (Pacer Doc. 1).
[23] *Id*. at 5–8.
[24] *Id*. at 9–10.
[25] Order, *LAI Sys.*, No. 1:18-CV-114, at 8–10 (Pacer Doc. 2-1).

information.[26] The defendants were ordered to comply with the COPPA Rule and to pay a $300,000 judgment as a civil penalty.[27]

The FTC's enforcement actions continue unabated. In late April, 2018, the FTC sent notice letters to two foreign companies that it suspected were collecting geolocation data from children.[28] The letters reminded the companies that COPPA applies to services directed at children in the United States. The letters "encourage[d]" compliance with the COPPA Rule.

About the Author:

Pierre Grosdidier is Counsel in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. Pierre divides his practice between construction litigation and construction contract drafting. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes litigating unauthorized computer access and software copyright infringement claims. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, and a registered P.E. in Texas (inactive).

[26] Complaint, No. 5:15-CV-2569, at 6, 10 (C.D. Cal., Dec. 17, 2015) (Pacer Doc. 1).

[27] Order, *Retro Dreamer*, No. 5:18-CV-114, at 8–10 (Pacer Doc. 2-1).

[28] Press Release, FTC Warns Gator Group, Tinitell that Online Services Might Violate COPPA (Apr. 27, 2018).

New Texas Cybersecurity Laws – Part 1

By Elizabeth Rogers and Aaron Gregg

The Texas Legislature considered and approved a variety of cybersecurity-related legislation during the 85th regular legislative session that went into effect on Sept. 1, 2017. Substantively speaking, Texas has taken a leadership role in addressing various cybersecurity and data privacy issues.

The Texas laws enacted in 2017 cover a wide range of relevant concerns, such as required practices for state agencies, continuous monitoring and auditing of network systems and processes, updating the penal code for the digital era, and important student data privacy protections. Other states have taken steps to address some of these issues, but the newly adopted Texas legislative approach is comprehensive. In this Part 1, we focus on the Texas Cybersecurity Act.

House Bill 8 by Rep. Giovanni Capriglione – "Texas Cybersecurity Act"

The Texas Cybersecurity Act establishes certain cybersecurity requirements for all state agencies in Texas, adds cybersecurity as an element of the sunset review process, creates a cybersecurity council, and requires that certain agencies conduct studies and reports related to cybersecurity threats and responses. House Speaker Joe Straus commented that the overarching goal of HB 8 is "to ensure state agencies are good stewards of private data."1

Consideration of Cybersecurity in Sunset Review Process

The Sunset Advisory Commission, an agency of the Texas Legislature, evaluates whether state agencies should be reformed, continued, or abolished, and makes recommendations to the Texas Legislature to that effect. When determining whether a public need exists for the continuation of a state agency, the Commission is now required to assess the agency's cybersecurity practices using information provided by the Department of Information Resources (DIR) or any other appropriate state agency. (Tex. Gov't Code § 325.011(14).)

Expanding the Role of the Texas DIR

HB 8 requires the DIR to develop and implement a plan to address cybersecurity risks and incidents in the state and authorized the agency to enter into an agreement, as needed, with an organization such as the National Cybersecurity Preparedness Consortium to support implementation efforts. (Tex. Gov't Code § 2054.076(b-1).) The DIR is also required to establish an "information sharing and analysis center" to provide a forum for agencies to share

information regarding cybersecurity threats, best practices, and remediation strategies. (Tex. Gov't Code § 2054.518.)

The Cybersecurity Act requires the DIR to provide mandatory guidelines to state agencies regarding the continuing education requirements for cybersecurity training to be completed by all information resources employees. (Tex. Gov't Code § 2054.076(b-1).) The DIR shall also establish the requirements for the biennial information security assessment and report that all state agencies must now conduct (discussed further below). (Tex. Gov't Code § 2054.515(c).)

Changes for State Agencies

Prior to passage of HB 8, state agencies were required to identify information security issues and develop a plan to prioritize the remediation and mitigation of those issues. This legislation adds specificity to that requirement by delineating five specific elements that an agency must consider when identifying the issues and developing the plan. (Tex. Gov't Code § 2054.575(a).)

Each state agency is now required to conduct an information security assessment of the agency's network systems, data storage systems, data security measures, and information resources vulnerabilities at least once every two years and to report the results to the DIR. (Tex. Gov't Code § 2054.515(a-b).) Similarly, each state agency shall submit a biennial data security plan to the DIR and conduct a vulnerability and penetration test of the agency's website and any mobile applications that process any personally identifiable or confidential information. (Tex. Gov't Code § 2054.516.)

Colleges and Universities

Institutions of higher education must adopt and implement a policy for websites or mobile applications operated by the institution to ensure that the privacy of individuals is protected and the confidentiality of information processed by the websites or applications is preserved. (Tex. Gov't Code § 2054.517.)

Open Meetings Act

The Texas Cybersecurity Act makes key changes to the state's Open Meetings Act. All governmental bodies in Texas will now be permitted to conduct closed meetings to deliberate network security assessments or deployments of security personnel, infrastructure, or devices. (Tex. Gov't Code § 551.089.) This new exception offers the freedom that an entity needs to properly deliberate these sensitive matters. Yet, any entity utilizing this provision must be

careful to limit such deliberations to the appropriate topic so as to not violate separate provisions of the Open Meetings Act.

Data Breaches

With respect to data breaches, HB 8 expands the categories of information that, if compromised, would trigger an agency's duty to notify affected individuals. (Tex. Gov't Code § 2054.1125(b).) HB 8 also adds an additional requirement that state agencies must now report a data breach or suspected data breach of system security to the DIR. (Tex. Gov't Code § 2054.1125(b).)

Another provision of the bill requires the Texas Secretary of State to conduct a study regarding cyberattacks on election infrastructure. The study must include an investigation of vulnerabilities in election infrastructure, information on any attempted cyberattack on a county's voting machines or registered voter lists, and recommendations for protecting voting machines and voter lists. (Tex. Elec. Code § 276.011.) The Secretary of State must prepare a public summary of the report as well as a confidential report for elected officials that will be exempt from disclosure under the Texas Public Information Act. (Tex. Elec. Code § 276.011.)

Cybersecurity Council & Select Legislative Committees

Cybersecurity Council

HB 8 requires the establishment of a Cybersecurity Council and specifies the make-up of the Council, which will be led by the state cybersecurity coordinator and will also include: representatives from the Offices of the Governor, the Lieutenant Governor, and the Speaker of the House of Representatives; private sector leaders; and representatives of institutions of higher education. (Tex. Gov't Code § 2054.512(a-c).) The Cybersecurity Council shall consider the costs and benefits of establishing a computer emergency readiness team, establish criteria for addressing cybersecurity threats, assess the knowledge, skills, and capabilities of the existing state cybersecurity workforce, consolidate and synthesize best practices, and provide recommendations to the legislature on legislation necessary to implement cybersecurity appropriate practices. (Tex. Gov't Code § 2054.512(d-e).)

Senate/House Committees on Cybersecurity

Finally, HB 8 calls for the creation of a Select Committee on Cybersecurity in both the House and Senate. Those Committees must, either jointly or separately, study the information security plans of each state agency and the risks and vulnerabilities of state agency cybersecurity.

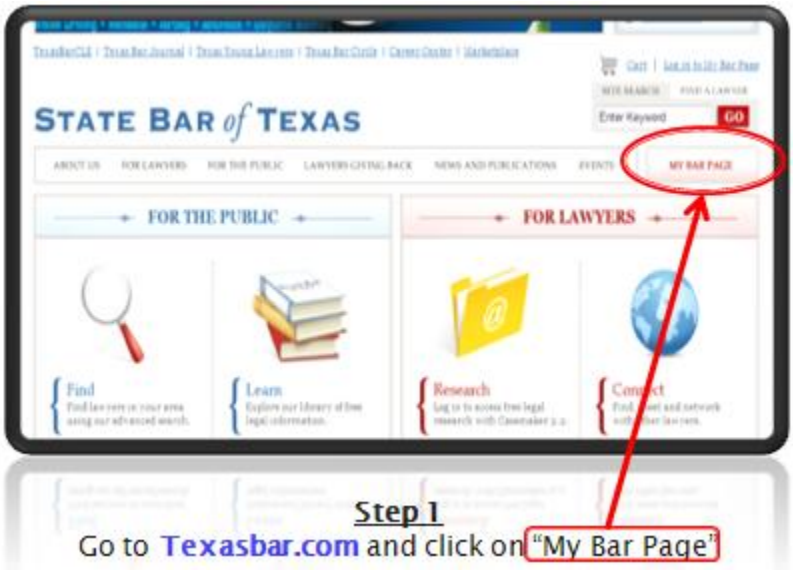
Practical Implications

The successful enactment of the Texas Cybersecurity Act shows that the state of Texas is serious about addressing cybersecurity as a matter of public policy. The Texas Legislature will be examining these issues closely via committees that will be formed and the reports and studies required by HB 8. The DIR has been given significant new responsibilities related to cybersecurity and will likely emerge as the go-to resource for such issues across Texas state government. The practical and immediate impact of HB 8 is that it will elevate information network and data security to be a top priority for a state agency or institution of higher education. And the Secretary of State will be hard at work ensuring that the state is following (and perhaps creating) adequate safeguards for our election infrastructure. Given the vast amount of confidential and/or personally identifiable information held by state agencies, this legislation provided a critical response to the ever-evolving cyber threats present today.

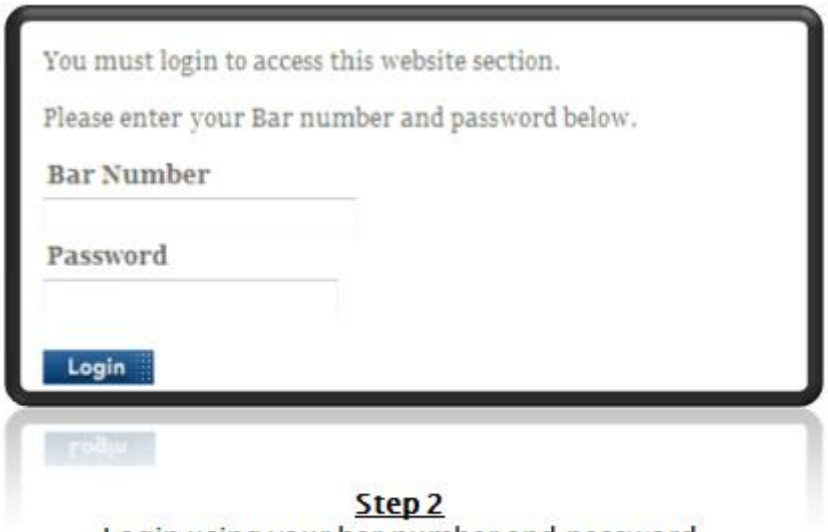
To effectively implement these new responsibilities, state agencies and institutions of higher education will need to develop reliable internal and external resources. It also will be important for state agencies and institutions of higher education to collaborate and coordinate among each other, and with the DIR, to sort through how best to comply with these myriad new responsibilities. Last, developing a network of subject matter experts will assist those impacted by HB 8 to comply with updated data breach notification procedures and Open Meetings Act exceptions.

How to Join the State Bar of Texas Computer & Technology Section

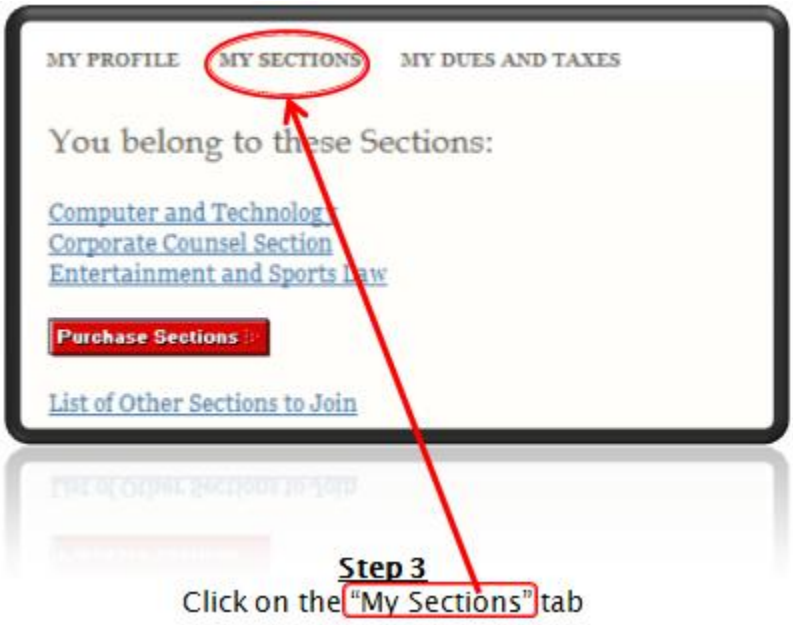
Joining the State Bar of Texas Computer & Technology Section is easy. You can join online by visiting the State Bar of Texas Website at www.Texasbar.com. Please follow these instructions to join the Computer & Technology Section online.



Step 1
Go to Texasbar.com and click on "My Bar Page"



Step 2
Login using your bar number and password
(this will be the same information you'll use to login to the Section website)



If you see "Computer and Technology", congratulations, you're already a member.

If not, click the "Purchase Sections" button and follow the instructions to add the Computer and Technology Section. **Please note: It may take several days for the State Bar to process your section membership and update our system.**

You can also complete this form and mail or fax it in.

State Bar of Texas Computer & Technology Section Council

Officers

Michael Curran – Austin – Chair
Sammy Ford IV – Houston – Chair-Elect
John Browning – Dallas – Treasurer
Shawn Tuma – Dallas – Secretary
Shannon Warren – Houston – Past Chair

Webmaster

Elizabeth Rogers – Austin

Term Expiring 2018

Pierre Grosdidier – Houston
David Coker – Dallas
Laura Leonetti – Houston
Reginald Hirsch – Houston

Term Expiring 2019

Sanjeev Kumar – Austin
Judge Xavier Rodriguez – San Antonio
Judge Scott J. Becker – McKinney
Eric Griffin – Dallas

Term Expiring 2020

Kristen Knauf – Dallas
Lisa Angelo – Houston
Rick Robertson – Plano
Eddie Block – Austin

Chairs of the Computer & Technology Section

2017-2018: Michael Curran
2016-2017: Shannon Warren
2015-2016: Craig Ball
2014-2015: Joseph Jacobson
2013-2014: Antony P. Ng
2012-2013: Thomas Jason Smith
2011-2012: Ralph H. Brock
2010-2011: Grant Matthew Scheiner
2009-2010: Josiah Q. Hamilton
2008-2009: Ronald Lyle Chichester
2007-2008: Mark Ilan Unger
2006-2007: Michael David Peck
2005-2006: Robert A. Ray
2004-2005: James E. Hambleton
2003-2004: Jason Scott Coomer
2002-2003: Curt B. Henderson
2001-2002: Clint Foster Sare
2000-2001: Lisa Lynn Meyerhoff
1999-2000: Patrick D. Mahoney
1998-1999: Tamara L. Kurtz
1997-1998: William L. Lafuze
1996-1997: William Bates Roberts
1995-1996: Al Harrison
1994-1995: Herbert J. Hammond
1993-1994: Robert D. Kimball
1992-1993: Raymond T. Nimmer
1991-1992: Peter S. Vogel
1990-1991: Peter S. Vogel