Contents

Note from the Chair

By Sammy Ford

Thank you for being a member of the Computer & Technology Section. We appreciate your support and membership, and are excited to share with you exciting new updates.

1. On December 7, we are holding our second annual legal tech CLE: With Technology and Justice for All. One year ago, the Houston area experienced the devastation brought by Hurricane Harvey. This year's CLE will especially highlight the ways in which lawyers and law firms can prepare for catastrophes. We will also host a reception in connection for our members.
2. I would also like to continue to highlight a benefit that is now in its third year – the Section's free online Techbytes. Our council continues to add additional topics, so check back frequently.
3. Finally, our Council welcomed four new members: Chris Downs, Seth Jaffe, Hon. Emily Miskel, and William Smith. It is also my pleasure to introduce you to the Co-Editors of Circuits: Pierre Grosdidier and Kristen Knauf. I encourage you look up, and stay in touch with, the members of the http://sbot.org/biographies.

I am excited for this bar year, and I believe our Section has a bright future. That future is bright because of our members and I encourage you to stay involved with the section and take advantage of its resources. We are constantly looking out for new benefits for our members, and I ask that if you have any suggestions for the Section please do not hesitate to email me directly: sford@azalaw.com.

Sammy Ford, Chair of the Computer and Technology Section 2018, State Bar of Texas

Letter from the Co-Editors

By Pierre Grosdidier and Kristen Knauf

Welcome to the first issue of *Circuits* for the 2018-19 bar year! The weather may be finally cooling off (wishful thinking, perhaps), but *Circuits* continues to cover several hot topics at the intersection of technology and law.

We start this issue with a five-year anniversary *In Memoriam* of the late Ralph Brock (1948-2013) by our Section's past Chair Jason Smith. Ralph looms large over the Texas State Bar in general, and our Section in particular, and we thank Jason for taking the time to remind us of his contributions.

While our section members were enjoying the 2018 State Bar of Texas Annual Meeting in Houston, the Supreme Court announced its decision in a landmark United States Supreme Court case concerning the privacy of historical cellphone location records. Ron Chichester gives us a detailed analysis of the Court's 5 to 4 decision in *United States v. Carpenter*.

Elizabeth Rogers and Aaron Gregg give us their Part 2 update on new Texas cybersecurity laws enacted during the 85th regular legislative session. New laws address cyber-attacks, ransomware, student privacy, and nuisance websites. Elizabeth is our new Secretary for 2018-19 bar year.

It is unfortunate that the concept of online bullying has become so prevalent that "cyberbullying" is now a legally defined term, distinct from other inappropriate forms of internet activity. Lisa Angelo takes a closer look at cyberbullying, and the growing legal protections and resources available to fight back against this digital scourge.

In the cyberbullying vein, is the recently-enacted Texas Revenge Porn Statute already dead on arrival? John Browning, our new Chair-Elect, reports on *Ex-Parte Jones*, the Tyler Court of Appeals' decision that holds that the statute impermissibly restricts free speech.

As legislators struggle to address the growing impact of cybercrime, we can expect additional cybersecurity requirements designed to defend of our economy and its many varied industries. Seth Jaffe, a new member of the Computer and Technology Section Council, examines various cybersecurity provisions that have been added to individual state breach notification laws.

Hannah Allison, the pro bono programs administrator for the Legal Access Division of the State Bar of Texas and manager of TexasLegalAnswers.com, explains why we should all RSVP "Yes"

to National Pro Bono Week. This year marks the tenth anniversary of National Pro Bono Week, October 22–26, 2018.

Finally, yours very truly reports on recent federal cases that have considered the constitutionality of cell phone border searches (spoiler: they are legal).

Many thanks all the contributors to this rich issue and for helping us keep this publication on schedule. Thank you also to Antony P. Ng and Elizabeth Rogers for their review of and assistance with this issue's articles. We hope that you enjoy reading *Circuits*, and welcome any comments that you may have: please send them to our section administrator at admin@sbot.org.

Kind Regards,

Pierre Grosdidier, Co-Editor

Kristen Knauf, Co-Editor

Five Years Later, *In Memoriam*: Ralph Brock (August 6, 1948–July 14, 2013)

By Jason Smith, Texas Computer and Technology Section Past Chair (2012–13)

On this 5th anniversary of the passing of our dear friend and colleague, it gives me great pleasure to announce that the State Bar of Texas Computer and Technology Section is renaming its Lifetime Achievement Award to the "Ralph Brock Computer & Technology Section Lifetime Achievement Award" and posthumously naming Ralph the 2018 recipient *in memoriam*.

I still remember receiving word of Ralph's passing. It was July 2013 and I had just completed my year as the Chair of the State Bar of Texas Computer and Technology Section, a role that began the previous year with Ralph passing me the gavel. Serving in the shadow of a State Bar of Texas legend, I did not take the responsibility lightly. Ralph had set the bar high. Not only in our Section, but in the many sections he had led. You see, Ralph was somewhat of a State Bar Section journeyman. A 1975 graduate of Texas Tech law school and a resident of Lubbock, Ralph found a way to serve the State Bar despite his geographical distance from the major population centers that tend to dominate the Bar activities. In addition to serving as Chair of the Computer and Technology Section, he served as the first Chair of the Individual Rights and Responsibilities Section—and even served as the only male Chair of the Women and Law Section! Ralph was soft-spoken and kind-hearted and seemed be incapable of making enemies. It was impossible to cross paths with Ralph and not feel immediately drawn to his motivating and loving presence. He was the kind of guy that makes writing these types of memorials difficult, simply because it can never be long enough, comprehensive enough, or do justice to a man who dedicated so much of himself to the service of others.

There was an outpouring of memories that came flooding in on news of Ralph's passing. Past Computer and Technology Section Chair, Mark Unger, a family law attorney from San Antonio remembered his last meal with Ralph this way:

*On **Thursday, June 20, 2013**, I sat across from Ralph Brock for the last time at our Computer Council dinner at Rathbun's Blue Plate Kitchen in Dallas, Texas. He ordered a perfect steak, while we all ordered whatever the waiter suggested and I watched the Spurs lose to the heat in game 7 on the flat-screen above his head. He knew what was important in life. He was a gentleman. He was a leader. He was our friend. His enjoyment of that meal in great company will forever be my consolation. It was the perfectly imperfect, as I had no idea it would be the last time together. No Council meeting will ever be the same and we are far lesser men and women for his passing. It was an honor to have known him in all ways. Rest in great peace, Ralph.*

Grant Scheiner, criminal defense attorney in Houston, and another past Chair of the Section remembers how Ralph was always encouraging and inspiring those around him:

One day, after presiding over a quarterly Section meeting, he took me aside and encouraged me to apply to become a Section Representative to the State Bar Board of Directors. I told him I would but later waffled, because it seemed like too great a time commitment. Then Ralph called me and told me it was a privilege to serve the Bar and doing so was "the greatest professional decision I have ever made." I hung up the phone and filled out my application immediately! Ralph always knew how to inspire others. He was the Knute Rockne of Texas lawyers.

D. Todd Smith, an appellate attorney from Austin and the President-elect of the Austin Bar Association, who followed Ralph as Editor of *The Appellate Advocate*, remembered Ralph as "extremely personable" and "ahead of his time." Others fondly remembered his intense curiosity about the law and his love for the Supreme Court. Ralph received both a Presidential Citation and a Certificate of Merit during the State Bar Annual Meeting just a month before his passing. The awards were recognition for "demonstrating exceptional service" and "outstanding contributions to the legal profession." The recognition was related to the pro bono Amicus Brief filed by the State Bar of Texas in *Trevino v. Thayer*, which Ralph drafted. That brief was referred to four times

during oral argument by Supreme Court Justices Kennedy and Breyer who propounded questions to counsel about the conclusions reached in the brief—a high compliment to Ralph's scholarship. It was also cited in the majority opinion.

We often hear people say that they hope to leave an organization, a community, or the world, itself, better than when they found it. Ralph left his mark on the State Bar of Texas, an impression on those of us fortunate to call him colleague and definitely left the world around him much better for simply having been a part.

New Texas Cybersecurity Laws – Part 2

By Elizabeth C. Rogers and Aaron Gregg

The Texas Legislature considered and approved a variety of cybersecurity-related legislation during the 85th regular legislative session. Each of the newly-enacted laws went into effect on Sept. 1, 2017. In Part 1, we discussed the highlight of the Texas Cybersecurity Act. In Part 2, we highlight the other laws the legislature enacted.

House Bill 9 by Rep. Capriglione – the Texas Cybercrime Act

The Texas Cybercrime Act is a response to the lack of clearly-defined criminal offenses related to cyberattacks, hacking, and other nefarious activity related to networks, devices, and digital information. The bill creates classes of criminal offenses for denial of service attacks, ransomware, and intentional deceptive data alteration.

Electronic Access Interference

The Cybercrime Act creates the offense of "Electronic Access Interference," a third degree felony. A person commits this offense by intentionally interrupting or suspending access to a computer system or network without the effective consent of the owner. Tex. Penal Code § 33.022(a)-(b). Importantly, the definition of this crime includes a defense to prosecution if the person who took an action described above did so with the intent to facilitate lawful access to a computer network or system for a legitimate law enforcement purpose. Tex. Penal Code § 33.022(c).

Electronic Data Tampering and Ransomware

HB 9 defines "Ransomware" as a computer contaminant or lock that restricts access, to an entire computer system or a computer file, by an unauthorized person to extort money from an authorized user and creates the offense of "Electronic Data Tampering." Tex. Penal Code § 33.023(a). A person commits this offense if the person: intentionally alters data as it transmits between two computers through deception and without a legitimate business purpose; or intentionally introduces ransomware onto a computer network or system through deception and without a legitimate business purpose. Tex. Penal Code § 33.023(b)-(c). The seriousness of this offense is dependent on the aggregate amount of financial losses involved, starting with a Class A misdemeanor for $100 or less and scaling up to a first degree felony for $300,000 or more. Tex. Penal Code § 33.023(d-1). The starting point is raised to a state jail felony for an amount of $2,500 or less if it is shown that the defendant knowingly restricted a victim's access to privileged information. Tex. Penal Code § 33.023(d-2).

This legislation is a positive step in the process of modernizing the Texas Penal Code and provides law enforcement agencies in Texas with more robust tools for fighting cybercrimes.

One key element of each of these new criminal statutes is the exception for legitimate business or law enforcement purposes. This important exception ensures that 'white hat' operations, internal network security testing conducted by a company on its own network or devices, or legal law enforcement activities do not unintentionally subject employees, contractors, or law enforcement personnel to criminal liability.

House Bill 2087 by Rep. VanDeaver – "Student Data Privacy Act"

After making a significant effort at passing similar legislation during the 2015 legislative session, Rep. VanDeaver succeeded this session in passing the Student Data Privacy Act. This important legislation provides strong privacy protections for student data within Texas public schools. Digital learning resources and internet-connected technology are transforming the classroom experience and the overall learning environment.

However, along with the many benefits that digital tools offer, there are also new risks that must be addressed, especially with respect to student data. HB 2087 struck a balance between addressing those risks while being careful not to stifle the benefits that these new digital tools offer. The legislation was based on a model student privacy law that had previously been enacted, with some variations, in at least 14 other states.

The Student Privacy Act prohibits the sale or rental of any student's data (Tex. Educ. Code § 32.152), bans targeted advertising to students based upon their use of educational services (*Id.*), and prohibits the use of a student's data to build a student profile for any purpose other than an educational purpose. *Id.* These important prohibitions protect students' privacy while still allowing the flow of data and information inherently necessary for the utilization of digital learning technology.

HB 2087 generally prohibits disclosure of student data, but also specifies when a third-party operator of an online service or application may permissibly disclose student data, including: to ensure legal or regulatory compliance; to protect against liability; to protect the safety and security of a website or application or the users of the website or application; for legitimate educational or research purposes; to comply with a request by the Texas Education Agency or a school district for a school purpose; with express consent of a student, to share data solely to provide access to employment, scholarships, or other educational opportunities for the student. Tex. Educ. Code § 32.153.

The Student Data Privacy Act also specifies for what purposes an operator may use a student's data, which is essentially limited to educational purposes and to improve educational products, but only if no data will be associated with an identifiable student. Tex. Educ. Code § 32.154.

Educational technology operators are also required to implement and maintain reasonable security procedures and practices designed to protect student data from unauthorized access, deletion, use, modification, or disclosure. Tex. Educ. Code § 32.155. Lastly, an operator must delete student data whenever a school or school district requests that the data be deleted, unless the student or student's parent consents to the operator's continued maintenance of the student's data. Tex. Educ. Code § 32.156.

Interactive websites and mobile applications have already changed the way that students, teachers, parents, and administrators interact with each other and the learning environment. These important privacy protections will allow such innovative technology to continue to thrive.

Senate Bill 1196 by Sen. Kolkhorst – the "Nuisance Website Act"

SB 1196 authorizes an individual, the Texas Attorney General, or a Texas district, county, or city attorney to bring a suit to declare that a person operating a web address or network of two or more computers is maintaining a common nuisance in certain circumstances. Tex. Civ. Prac. & Rem. Code § 125.0025.

Nuisance Website Act actions may be brought under the Texas Civil Practice and Remedies Code against a person operating a web address engaging in: organized criminal activity as a member of a combination as prohibited by the Penal Code; prostitution, promotion of prostitution, or aggravated promotion of prostitution; compelling prostitution; sexual assault; aggravated sexual assault; continuous sexual abuse of a young child or children; massage therapy or other massage services in violation of Chapter 455, Occupations Code; or any other activity operating on a web address, the business of which is the offering of a service or the selling, renting, or exhibiting of items intended to provide sexual stimulation or sexual gratification to the customer; trafficking of persons; sexual conduct or performance by a child; or employment harmful to a child. Tex. Civ. Prac. & Rem. Code § 125.0015(c), (d).

This legislation represents a novel attempt to combat human trafficking through innovative means and by extending the already-existing framework of nuisance law into the digital arena. The bill was crafted with the goal of substantially slowing down the rapidly-increasing use of websites and digital platforms to facilitate the practice of human trafficking. Law enforcement agencies now have an expanded arsenal of civil tools to shut down portals to criminal activity.

Attorneys experienced in nuisance actions should be aware of this novel application of nuisance law.

House Bill 3593 by Rep. Bernal – "Cybersecurity Education Act"

The Cybersecurity Education Act, which went into effect on May 15, 2017, requires the State Board of Education to allow public school districts to offer cybersecurity courses for credit for high school graduation and to create language credits for coding courses. Tex. Educ. Code § 28.002(f)(2); 28.025(b-12). In addition, a school district may offer a course about cybersecurity issues for credit without State Board approval if it partners with one or more institutions of higher education to develop and provide the course. Tex. Educ. Code § 28.002(g-1).

The Act expands the New Instructional Facilities Allotment to renovate existing facilities for cybersecurity labs (Tex. Educ. Code § 42.158.), moves technical application courses under career and technical education (CTE) (Tex. Educ. Code § 42.154(b).), gives teachers a CTE certification subsidy, and lists cybersecurity and coding under the Science, Technology, Engineering, and Mathematics (STEM) endorsement options. Tex. Educ. Code § 28.025(c-10); 29.190(b).

HB 3593 is an important step towards ensuring that the public education system in Texas is producing students equipped to be part of a 21st century workforce. Understanding the various elements of cybersecurity and how to code are crucial skills for many jobs that exist today and even more that will exist in the future. The technology sector has grown by leaps and bounds in Texas in recent decades, and creating a pipeline of students that are familiar with cybersecurity and coding is a key element to continuing that growth.

About the Author

This Article was prepared by **Elizabeth C. Rogers**, Privacy & Cybersecurity Partner at Michael Best & Friedrich, LLC and **Aaron C. Gregg**, Associate in the Government, Law and Policy Practice Group at Greenberg Traurig, LLP. Elizabeth was the first Chief Privacy Officer in Texas State Government and has first-hand experience working with the Texas Department of Information Resources in developing a state agency cybersecurity and privacy division. Aaron has more than a decade of experience, before and after law school, in working at the Texas State Capitol, including advising clients concerning privacy legislation.

Carpenter v. United States: The Supreme Court Hands Privacy Advocates a (Limited) Victory

By Ron Chichester, Texas Computer and Technology Section Past Chair

In *Carpenter v. United States*, No. 16-402, 585 U.S. ___ (2018), the U.S. Supreme Court ruled that the government must get a warrant to obtain certain types of information from cell-phone providers.

1. The Facts

There were a series of robberies at several different Radio Shacks and T-Mobile stores in the greater Detroit area (covering locations in both Michigan and Ohio). The FBI nabbed a suspect, who later confessed and turned informant. In doing so, the informant identified fifteen accomplices and provided phone numbers for some of the fifteen. The FBI then performed an examination of the informant's phone and culled additional phone numbers beyond the fifteen identified. It is not clear from the Court's opinion whether Carpenter was one of the original fifteen identified by the informant, or if Carpenter's phone number was simply among the additional numbers culled by the FBI.

Subsequently, the FBI obtained two court orders from two federal magistrates for Carpenter's cell site location information ("CSLI") under the Stored Communications Act, 18 U.S.C. §2703(d) (the "SCA").

> "The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records covering the period when Carpenter's phone was "roaming" in northeastern Ohio. Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day." (Pp. 3.)

Of the multitude of suspects arrested, seven pegged Carpenter as the ringleader. Carpenter was charged with twelve counts total for six of the robberies. Carpenter moved to suppress the CSLI evidence, citing an expectation of privacy in the cell phone data. The district court denied the motion. Subsequent expert testimony placed Carpenter "right where the . . . robbery was at the exact time of the robbery." P. 3, citing App. 131 (closing argument). Carpenter was convicted on eleven of the counts and sentenced to 100+ years in prison. The Sixth Circuit, claiming that Carpenter "shared" the location information with the respective telecommunications providers, affirmed under the third party doctrine. 819 F.3d 880 (6th Cir.

2016) (citing *Smith* v. *Maryland*, 442 U.S. 735, 741 (1979)). The third party doctrine states that there is no expectation of privacy when the information is "shared" with a third party, in this case, the telecommunications provider.

2. The Opinion

The Supreme Court, in a 5-4 decision, reversed. Chief Justice Roberts sided with the Court's four "liberals" and wrote a unified majority opinion (no concurrences). The dissent was as fractured as Eagle Ford, with each of the four "conservatives" writing their own dissenting opinions.

The majority focused on four areas: the Fourth Amendment & technology (pp. 4-15), the third party doctrine (pp. 15-17), the limitations of the opinion (17-18), and the standards for CSLI and the SCA (pp. 18-22).

The one-sentence summary of the case is: The government can get spying data, but not too much of it without a warrant. In other words, there are limitations on data fishing expeditions by the government. This is actually in tune with standard e-discovery practice, but is seemingly at odds with the third party doctrine previously promulgated by the Court itself. Is the third party doctrine dead? No, said the Court, but that doctrine must be sensitive to cultural use of technology and the implications of that technology in view of the original intent of the Fourth Amendment.

After a quick review of Fourth Amendment jurisprudence (pp. 4-6), the Court touched on the balance between the need for government surveillance capabilities and the privacies expected when the Fourth Amendment was adopted (pp. 5-7). Importantly, the majority opinion cited Justices Alito's and Sotomayor's concurring opinions in *United States v. Jones*, 565 U.S. 400 (2012) (the GPS tracking case), as well as *Katz* v. *United States*, 389 U.S. 347, 351 (1967) ("the Fourth Amendment protects people, not places").

What technology trips Fourth Amendment protection? The Court wasn't clear on that point. The dissent (particularly Justice Kennedy) said that there was no rubric in this case that prompted Fourth Amendment protection. The majority averred, stating that "[a]lthough no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." Pp. 5-7, citing *Carroll v. United States*, 267 U.S. 132, 149 (1925). Perhaps to stave off the dissent, or for whatever reason, the majority distinguish cell-phone tracking information from other technologies heretofore considered by

the Court. (Pp. 6–7.) Repeatedly, and importantly, during the recitation of precedent, the Court focused on the character of the information (location or otherwise of the person) as well as the amount of information gathered.

In short, when participation in conventional society prompts the use of a technology that:

- requires the cooperation of a third party; and
- generates information about the person that would come under the purvey of the Fourth Amendment but for that third party,

then strict adherence to the third party doctrine is (pardon the pun) unwarranted.

Culture is all about communication. Historically, people adopt tools to facilitate communication, and those tools become part of that culture. The Supreme Court merely recognizes a Twenty-First Century cultural form that, if it had been available to the Founders, would doubtlessly have been within the rubric of the Fourth Amendment. Such juxtaposition is fraught with difficulty, but it appears that the Supreme Court feels that it is worth the effort. Maybe they will come up with a name for this new doctrine, something like the "inherent sharing doctrine."

About the Author

Ronald Chichester is a solo practitioner in Tomball who specializes in technology-related legal issues. He is past chair of both the Business Law Section and the Computer & Technology Section. Ron is a former adjunct professor at the University of Houston where he taught courses in computer crime and e-commerce. He is a registered patent attorney, a certified computer forensics examiner and a certified information systems auditor. Ron received his JD from the University of Houston and he holds a bachelors and a master degree (both) in aerospace engineering from the University of Michigan.

Expect warrantless digital device searches at the border

By Pierre Grosdidier – Haynes and Boone, LLP

Over the last decade, travelers have occasionally recounted the travails that they encounter entering the United States with their smart phones and laptops. Journalists tend to make the top of the lists of border digital searches—and the headlines—but they are by no means the only ones. The U.S. Customs and Border Protection ("CBP") reports on its website that it searched the devices of 30,200 travelers in 2017, or approximately 0.007 percent of the more than 397 million travelers who arrived to the U.S. from abroad that year.[1] Even though digital border searches are manifestly rare, they are particularly problematic for attorney, whose digital devices might contain confidential and privileged client information. But despite the Supreme Court's landmark *United States v. Riley* decision, recent developments indicate that border digital searches will continue largely unimpeded. In *Riley*, the U.S. Supreme Court held that the Fourth Amendment's ban on unreasonable searches meant that warrantless searches of cell phones seized incident to an arrest were unconstitutional, absent exigent circumstances.[2]

It is well established that the sovereign's interest in territorial integrity reaches its zenith at the border.[3] Accordingly, the "border search" exception to the Fourth Amendment's protections dispenses CBP officers from securing probable cause-based warrants for border searches, either inbound or outbound.[4] International travelers' expectation of privacy is thus greatly reduced, and what protections remain generally apply to persons, not their property.[5] The touchstone of what warrantless searches are allowed is reasonableness.[6] The Supreme Court has defined reasonable suspicion as "a particularized and objective basis for suspecting the

---

1 Press Release, CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics (Jan. 5, 2018).

2 *Riley*, 134 S.Ct. 2473, 2494-95 (2014). The *Riley* arrests were domestic, not at the border. The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV.

3 *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004).

4 *United States v. Ramsey*, 431 U.S. 606, 619 (1977); *United States v. Kolsuz*, 890 F.3d 133, 137 (4th Cir. 2018) ("we have long held that the rationales underlying the border exception extend to exit as well as entry searches").

5 *United States v. Vergara*, 884 F.3d 1309, 1312 (11th Cir. 2018) ("we require reasonable suspicion at the border only 'for highly intrusive searches of a person's body such as a strip search or an x-ray examination.'").

6 *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013).

particular person stopped of criminal activity," an analysis that must consider "the totality of the circumstances."[7]

The border search exception applies equally to digital devices, which the CBP regards as luggage. The key issues as to these devices are the level of the search, *i.e.*, basic versus forensic, and the level of suspicion of illicit activity required for each, *i.e.*, none or a reasonable level of suspicion. No court has held that reasonable suspicion is required for a basic search, which means that CBP officers are free to manually rummage through a traveler's cell phone or computer.[8] Federal appellate courts are split regarding the level of suspicion required for forensic searches.

In *United States v. Kolsuz*, CBP officers detained departing traveler Kolsuz after they found unauthorized firearm parts in his suitcases.[9] The CBP seized and forensically searched his phone. Kolsuz was ultimately convicted and appealed the district court's denial of his motion to exclude the evidence collected from his iPhone. Invoking *Riley*, and the fact that the forensic search took a month, at a place "miles away from [the] airport," and after his arrest, Kolsuz argued that the grounds for the border search exception no longer applied and that his iPhone's forensic search required "a warrant based on probable cause."[10] The Fourth Circuit Court of Appeals disagreed, holding that the delayed, off-site forensic search remained a border search because of its nexus to the contraband firearm parts.[11] But the court held that, because of its invasiveness and especially in light of *Riley*, the forensic search qualified as a "nonroutine border search, requiring some measure of individualized suspicion."[12] The court also held that CBP officers reasonably relied on the assumption that the reasonable suspicion standard justified their search of Kolsuz's iPhone. The Court, therefore, did not have to decide whether the search required more than reasonable suspicion and it affirmed Kolsuz's conviction.

---

7 *Id.* at 968 (citing *United States v. Cortez*, 449 U.S. 411, 417–18 (1981)).

8 *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) ("[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant"); *Cotterman*, 709 F.3d at 960–61 (as applied to electronic devices).

9 *Kolsuz*, 890 F.3d 133, at 136.

10 *Id.* at 140, 142.

11 *Id.* at 142–43.

12 *Id.* at 137, 144–45.

Kolsuz's holding is consistent with the Ninth Circuit Court of Appeals' *United States v. Cotterman* decision.[13] Border agents seized Cotterman's digital devices when he entered the United States from Mexico based on his 15-year old child molestation conviction. A basic search found personal photos and password-protected files, and later off-site forensic searches found hundreds of photos and videos of child pornography. Using privacy arguments similar to those later invoked by the Supreme Court in *Riley*, the court held that a forensic search at the border required reasonable suspicion.[14] The court further held that the forensic searches in this case were reasonable in light of the totally of the circumstances, namely Cotterman's prior conviction, his frequent out-of-country travels, his return from Mexico ("a country known for sex tourism"), and his locked files.[15]

But recently, in *United States v. Touset*, the Eleventh Circuit Court of Appeals held that forensic border searches did not require reasonable suspicion.[16] Touset's digital devices were seized when he entered the country based on the suspicion that he was involved in child pornography overseas. Forensic searches found child pornography on four devices. Touset pleaded guilty but reserved the right to appeal the trial court's denial of his motion to suppress the forensically-collected evidence.[17] The court of appeals affirmed. It noted that the Supreme Court "never required reasonable suspicion for a search of property at the border, however non-routine and intrusive," and saw no reason to hold otherwise.[18] The court also saw no reason to treat digital devices differently from physical luggage. It found unpersuasive the reasoning in *Kolsuz* and *Cotterman* because it had already held in *United States v. Vergara* that *Riley* did not apply to border searches.[19] In the alternative, the court affirmed because border agents had reasonable suspicion to forensically search Touset's digital devices.[20]

These three decisions lend judicial support to the CBP's 2018 Border Search of Electronic Devices Directive, which authorizes digital device searches at the border, either inbound or outbound.[21] Searches are limited to information on the device, and CBP officers "may not

---

[13] 709 F.3d at 957.
[14] *Id.* at 968.
[15] *Id.* at 968-69.
[16] 890 F.3d 1227, 1232-33 (11th Cir. May 23, 2018).
[17] *Id.* at 1230-31.
[18] *Id.* at 1233.
[19] *Id.* at 1234 (citing *Vergara*, 884 F.3d at 1312).
[20] *Id.* at 1237.
[21] CBP Directive No. 3340-049A, *Border Search of Electronic Devices*, Jan. 4, 2018.

intentionally use the device to access information that is solely stored remotely."[22] Thus, officers may scroll through device-resident picture folders, web browser histories, and downloaded emails, but remote information, like emails and banking records not downloaded, are off limits. Practically speaking, a search can be confined to the device by disabling its network connectivity, as required by the Directive.[23] Simply placing the phone in airplane mode will disable its network connectivity.

CBP officers may perform basic device searches with or without suspicion.[24] Advanced searches performed by accessing devices electronically require reasonable suspicion of illicit activity and a supervisor's presence.[25] Of course, as the *Kolsuz* court noted, this reasonable suspicion standard is not necessarily constitutionally required.[26] And in fact, the CBP may convey seized devices to U.S. Immigration and Customs Enforcement, which is not limited by the Directive's terms.[27]

Under the Directive, CBP officers should inspect devices in the presence of their owners, unless a reason justifies otherwise. Travelers can be asked to provide passwords or to decrypt protected files, and inaccessible devices can be detained.[28] The Directive includes an arguably cumbersome procedure for handling legally privileged information.[29] Confidential business and commercial information enjoys some level of protection from disclosure. But the Directive states that "the existence of a relevant national security-related lookout in combination with other articulable factors as appropriate" may create the reasonable suspicion required for a forensic search.[30] This test is less stringent that the Supreme Court's own "particularized and objective basis" criterion. As the Supreme Court held in *Cortez*, "[t]erms like 'articulable reasons' and 'founded suspicion' [to authorize police stops] are not self-defining; they fall short of providing clear guidance dispositive of the myriad factual situations that arise."[31]

---

[22] *Id*. at 4.
[23] *Id*.
[24] *Id*.
[25] *Id*. at 5.
[26] *Kolsuz*, 890 F.3d at 146.
[27] CBP Directive at 2.
[28] *Id*. at 5-6.
[29] *Id*. at 6.
[30] *Id*. at 5.
[31] *Cortez*, 449 U.S. at 417.

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 data privacy, unauthorized computer access, and media and entertainment issues and litigation. 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).

Legal Protections Against Cyberbullying

By Lisa M. Angelo

"Cyberbullying" is a term that has gained notoriety as it is more common for people of all ages to interact online. The increase in social media outlets, online gaming, and use of mobile devices has cultivated prime conditions for cyberbullies to reign terror. You can often spot a bully "trolling" in the comments section of an online post; a trail of extreme or offensive comments that lead one to presume all sense of humanity may be lost. Those brave enough to continuing reading along the trail will find that the slightest hint of a defense serves only to fuel the troll.

The concept of online bullying has become so prevalent that "cyberbullying" is a legally defined term, distinct from other inappropriate or undesired forms of cyber-related activity. According to the Texas Education Agency, the term "cyberbullying" refers to actions involving minors only.[1] Terms that apply to activity involving an adult on either side of the victim-bully relationship is referred to as "cyber-harassment" or "cyber-stalking".[2] Victims of adult-aged bullies (over the age of eighteen) will need to look to other laws for protection and legal recourse.[3]

Cyberbullying differs from in-person bullying because, in the cyberworld, a bully has almost unlimited interaction and access to the victim via constant internet connection(s) and mobile devices. For children, the bullies' interactions are not limited to school hours because communication portals are open throughout the evening and weekends. It is common for children to have continuous access to an internet connection. According to a study in the UK, 86% of children ages twelve to fifteen had mobile devices in 2017.[4] The result of constant connection can mean constant bullying; messages are spread and shared instantaneously across the internet. The reality of the matter is that even if the child disconnects from the internet, the bullying can continue. The messages can continue to spread, only to be discovered when the child logs back in or attends class the next day.

---

1 Texas Education Agency, https://tea.texas.gov/Texas_Schools/Safe_and_Healthy_Schools/Coordinated_School_Health/Coordinated_School_Health_-_Bullying_and_Cyber-bullying/ (last visited Aug. 17, 2018).

2 *Id.*

3 Other laws to consider include the Texas Penal Code Ch. 33 or Chapter 42.

4 Statista, https://www.statista.com/statistics/398283/children-regular-use-of-mobile-phones-by-age-uk/ (last visited Aug. 17, 2018).

In 2016, suicide was the second cause of death for children ages ten to twenty-four.[5] While there may be many factors influencing a young person to take his or her own life, cyberbullying can detonate the situation.[6]

Because cyberbullying is performed via internet or text messages, and often off campus, it has been especially challenging for schools to address the problem. Schools typically lacked authority to intervene in activities that occurred off campus. In the 85th Legislature, Texas lawmakers passed an Act, effective September 1, 2017, that gives schools a mechanism to address cyberbullying. The Act amended several laws including Section 37.0832 of the Education Code to specifically address cyberbullying in public schools.[7] Not only does this Act, known as "David's Law," allow public schools to reach beyond the playground, it also provides legal recourse and criminal consequences for cyberbullying.[8]

David's Law expands the definition of "bullying" to include "cyberbullying" which means "bullying that is done through the use of any electronic communication device, including through the use of a cellular or other type of telephone, a computer, a camera, electronic mail, instant messaging, text messaging, a social media application, an internet website, or any other internet-based communication tool."[9] David's Law also brings cyberbullying that occurs outside of school property or school-related activity within the school's jurisdiction.[10] However, to expand beyond the school, the cyberbullying must interfere with the student's educational opportunities or substantially disrupt school activity.[11]

In addition to defining cyberbullying and broadening the school's jurisdiction, David's Law also requires school districts develop policies and procedures that incorporate items such as:

- Notice of cyberbullying to the alleged victim's parents/guardians within 3 days;
- Notice of cyberbullying to the alleged bully's parents/guardians;

---

5 "10 Leading Causes of Death by Age; National Vital Statistics System", https://www.cdc.gov/injury/wisqars/pdf/leading_causes_of_death_by_age_group_2016-508.pdf.

6 Centers for Disease Control & Prevention, "Suicide: Risk & Protective Factors", https://www.cdc.gov/violenceprevention/suicide/riskprotectivefactors.html.

7 David's Law.

8 *Id.*

9 David's Law; Texas Education Code §§ 37.0832; 12.104(b).

10 *Id.*

11 *Id.*

- Intervention & Counseling Options; and
- Procedures to anonymously report cyberbullying.[12]

David's Law permits the school to use its discretion in disciplining, up to and including expulsion of students who engage in bullying that is violent, suicide-enticing, or involves intimate visual material.[13] There is some protection for the schools, school personnel, and volunteers from liability when exercising their discretion. This protection also covers the decision to report an incident to law enforcement.[14]

Victims of cyberbullying may seek injunctive relief under Section 129A of the Education Code. The victim is entitled to a TRO upon showing likely success in establishing the defendant cyberbullied the victim.[15] It is a fairly low-burden of proof because the victim is not required to plead or prove immediate and irreparable harm. When the court grants the injunctive relief, it may, either on motion or *sua sponte*, order the preservation of relevant electronic communication.[16]

Along with injunctive relief, cyberbullies may face criminal liability. David's Law amends Section 42.07(c) of the Texas Penal Code to raise cyberbullying charges to a Class A misdemeanor in some situations.

In March 2017, a couple was arrested in Galveston, Texas for online bullying that had resulted in a teen suicide.[17] Charges were filed against the couple prior to the adoption of David's Law. With David's Law on the horizon, many speculated as to whether the couple could be prosecuted pursuant to David's Law. One of the defendants was initially charged with a Class A misdemeanor for publishing or threatening to publish intimate visual material[18], also known as a violation of the Revenge Porn Statute[19]. Now that David's Law has passed, it is unlikely to

---

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *State of Texas v. Andres Arturo Villagomez*, No. MD-0371485, County Court at Law No. 1 (March 16, 2017).

[18] *Id.*

[19] The "Revenge Porn Act" is also known as the Relationship Privacy Act. It created both civil and criminal liability under the Texas Penal Code Chapter 21.16. However, an appellate court in Tyler, Texas, recently ruled that the Revenge Porn Act was overly broad and violated the First Amendment. The issue has not yet been raised in the Galveston criminal case and civil liability might still be available.

apply in this case because the individuals accused of bullying were over the age of eighteen. It is also unclear if David's Law could apply retroactively. However, the defendants may still face other charges because other areas of the penal code will likely apply to the situation. The case is ongoing.

In summary, when dealing with cyberbullying of school-aged children, you should look to the Texas Education Code and David's Law for possible injunctive relief and criminal liability. Also, refer to the public- school district's policy on cyberbullying. Some courts have forms available for guidance when filing cyberbullying cases.

Below is an overview of ways in which David's Law amends the Texas Education Code:

- Defines "cyberbullying";
- Applies to off campus activity;
- Provides injunctive relief;
- Implements criminal consequences for cyberbullying; and
- Demands school districts implement policies & procedures to address cyberbullying.

Hopefully, the effect of David's Law on school policies will be helpful to proactively deter cyberbullying and reduce rates of suicide among youth.

Resources on cyber-bullying in Texas:
https://tea.texas.gov/Texas_Schools/Safe_and_Healthy_Schools/Coordinated_School_Health/Coordinated_School_Health_-_Bullying_and_Cyber-bullying/

http://www.davidslegacy.org/wp-content/uploads/2017/10/Davids-Law-One-Pager-R2.pdf

Research:
http://www.edtechpolicy.org/cyberk12ARCHIVE/Documents/C3Awareness/C3_framework_full_final.pdf

2012 Article on Cyberbullying
https://www.elon.edu/docs/e-web/academics/communications/research/vol3no1/04DoneganEJSpring12.pdf

School Policy on cyberbullying
http://bartonps.vic.edu.au/wp-content/uploads/sites/140/2017/12/Student-Engagement-policy.docx.pdf

Guidance Counselor Handling Bullying
http://www2.uwstout.edu/content/lib/thesis/2011/2011pagelk.pdf

Nansel TR, Overpeck M, Pilla RS, Ruan WJ, Simons-Morton B, Scheidt P. Bullying Behaviors Among US Youth: Prevalence and Association With Psychosocial Adjustment. *JAMA : the journal of the American Medical Association*. 2001;285(16):2094-2100.

https://txssc.txstate.edu/featured/

http://www.davidslegacy.org/davids-law/

https://tea.texas.gov/Texas_Schools/Safe_and_Healthy_Schools/Coordinated_School_Health/Coordinated_School_Health_-_Bullying_and_Cyber-bullying/

https://capitol.texas.gov/tlodocs/85R/analysis/html/SB00179F.htm

About the Author

Lisa M. Angelo is an attorney focused on helping businesses mitigate and manage cyber liability. She advises clients on data privacy, cybersecurity, business transactions, and other areas related to cyber law. Lisa also has a strong background in insurance law and helps clients with cyber insurance disputes. Lisa is the founding attorney of a forward-thinking, "virtual" law practice. She is an elected council member for the State Bar of Texas Computer & Technology Section. She also serves as the Vice-Chair of the State Bar of Texas Business Law Section's General Practice Committee and is a member of the Blockchain Committee. In addition, she is a member of the FBI's InfraGard Houston Chapter. Lisa is a Certified Information Privacy Manager and licensed to practice law in Texas and Colorado. She earned a Juris Doctorate from South Texas College of Law and a bachelor's in psychology from The University of Texas at Austin.

The Texas Revenge Porn Law: On Life Support After *Ex Parte Jones?*

By John G. Browning

In 2015, Texas took a giant step forward in combating one of the darkest byproducts of the Digital Age: "revenge porn," the term commonly ascribed to the sharing or online posting of sexually explicit images of individuals without their consent. That year, the Texas Legislature joined more than two dozen other states by passing the Relationship Privacy Act, which not only criminalized revenge porn but also set forth civil remedies for such conduct as well. But in April 2018, Tyler's 12th Court of Appeals pronounced the statute unconstitutional in *Ex Parte Jordan Jones*. This article will provide a brief overview of both Texas' revenge porn law as well as the case that struck it down.

Revenge porn sits squarely at the nexus of innovations in technology and a shift in social mores. Aided by digital advances and widely-used platforms and applications like Snapchat, it has become frighteningly easy for individuals to consensually share intimate photos or videos with a partner. But when a current or former partner or spouse decides to publish or disseminate such images to third parties without the consent of the person depicted (often motivated by anger over a breakup, a perceived wrong, or even jealousy of the ex's new relationship), the crime of revenge porn is born. The Cyberbullying Research Center estimates that there are as many as 2,000 revenge porn websites worldwide, while the Data & Society Research Institute reports that about one in twenty-five Americans have either been threatened with or victimized by nonconsensual image sharing. And, while women are much more likely than men to be victimized in this way, revenge porn has claimed victims across all walks of life and both genders—students, office workers, professionals, and even celebrities like actress Jennifer Lawrence or supermodel Kate Upton. Even politicians like Texas Congressman Joe Barton have fallen prey to revenge porn. Often, victims' images are not the only thing shared, as spiteful exes frequently include identifying information such as names, contact information, and links to their social media profiles. Victims have been threatened with sexual violence, stalked, harassed, fired from jobs, forced to move or change schools. A number have even committed suicide.

Prior to the passage of the revenge porn statute in Texas, victims sought criminal and civil relief using existing laws involving harassment, online impersonation, invasion of privacy/intrusion upon seclusion, and even defamation. See, for example, *Rauhauser v. McGibney*, 2014 WL 6996819 (Tex. App.—Fort Worth 2014, no pet.); *GoDaddy.com, LLC v. Toups*, 429 S.W.3d 752 (Tex. App.—Beaumont 2014, pet. denied). But in 2015, at the behest of

State Senator Sylvia Garcia of Houston, the Texas Legislature passed S.B.1135, the Relationship Privacy Act, which after being signed into law, became Section 21.16 of the Texas Penal Code.[1]

Under the law, a person commits an offense if "the person intentionally threatens to disclose, without the consent of the depicted person, visual material depicting another person with the person's intimate parts exposed or engaged in sexual conduct" and the actor "makes the threat to obtain a benefit: (1) in return for not making the disclosure; or (2) in connection with the threatened disclosure." The statute goes on to define "visual material" as "any film, photograph, videotape, negative, or slide or any photographic reproduction that contains or incorporates in any manner any film, photograph, videotape, negative, or slide; or any disk . . . or other physical medium that allows an image to be displayed on a computer or other video screen" and "any image transmitted . . . by telephone line, cable, satellite transmission, or other method." Pursuant to the statute, it is not a defense that a person depicted either created or consented to the creation of the visual material, or even that he or she voluntarily transmitted the material.

Violations of the Relationship Privacy Act are Class A misdemeanors punishable by up to a year in jail and a fine of up to $4,000. The statute also provides civil remedies for victims including injunctive relief (to halt the dissemination of images), as well as actual damages (including damages for mental anguish), reasonable attorney's fees, and court costs. And as far as the class of defendants targeted by this law is concerned, the Act not only sought to punish the individual who shared or threatened to share the intimate images of a former partner, but also third parties—such as revenge porn sites themselves—who might promote or profit by the unauthorized disclosure of these images. The Act provides for liability "for damages arising from the promotion of the material if, knowing the character and content of the material, the defendant promotes intimate visual material . . . on an internet website or other forum for publication that is owned or operated by the defendant." "Promotion" was given a particularly broad meaning, encompassing "to procure, manufacture, issue, sell, give, provide, lead, mail, deliver, transfer, transmit, publish, distribute, circulate, disseminate, present, exhibit, or advertise."

---

[1] Senator Garcia's office reached out to several members of the Computer & Technology Section Council, including the author. Over the course of multiple conference calls and emails, these Council members provided Senator Garcia's staff with considerable input and proposed draft language, including language from other states' revenge porn laws that had passed constitutional muster. For reasons unknown, these suggestions were not followed.

Although a number of civil lawsuits and criminal prosecutions of revenge porn cases have occurred statewide both before and since the passage of the Relationship Privacy Act, its sternest test took place earlier this year. After posting the nude photo of a woman online, Jordan Bartlett Jones was charged with violating Section 21.16(b) of the Texas Penal Code. When his pretrial application for writ of habeas corpus challenging the statute on First Amendment grounds was denied by the trial court, Jones appealed to Tyler's 12th Court of Appeals. On April 18, 2018, that appellate court declared the Relationship Privacy Act unconstitutional, finding it to be overly broad, vague, and having the potential to violate the rights of third parties who might unwittingly share intimate depictions of someone.

The Court began with its First Amendment analysis, observing that because photographs and visual recordings are inherently expressive, freedom of speech was clearly implicated. Next, its analysis shifted to whether the speech in question was content-based or content-neutral, and finding that the speech was content-based, the Court noted that any restriction would be subject to strict scrutiny. The court held that while the state purported to serve a compelling government interest—protecting privacy rights—the real problem lay in the language of the statute, which did not use the least restrictive means of serving that government interest. As the Court pointed out, the disjunctive wording of the law resulted in a person who shared the intimate images blissfully unaware of the circumstances under which they were created being subject to the same punishment as someone who had knowingly and intentionally violated the victim's privacy rights. The Court illustrated this with a hypothetical in which a "revenge porn" image is disseminated not only by a vengeful ex-boyfriend, but also by a friend of the boyfriend who has never met the victim. Having no cause to recognize her or to know the nonconsensual context in which her image was shared, this more distant friend shares the image with several individuals including a co-worker of the girlfriend. Should this unwitting friend be subject to prosecution like the spiteful ex-boyfriend? The appellate court was troubled that such a person "nonetheless is culpable despite his having no knowledge of the circumstances surrounding the photograph's creation or the depicted person's privacy expectation arising thereunder."

In addition to finding the statute to be an invalid content-based restriction on free speech, the Tyler Court of Appeals also found that the Act itself was constitutionally overbroad. Noting how modern technology has made the "daily sharing of visual material" "almost ritualistic," the Court opined that the statute "violates rights of too many third parties by restricting more speech than the Constitution permits." Accordingly, the appellate court reversed and remanded.

So in the aftermath of *Ex Parte Jones*, what is the fate of Texas' revenge porn statute? While the Tyler court's ruling is technically binding authority only on the dozen or so northeast Texas counties within the 12th District, it is the only appellate court to have considered this law and therefore is likely to constitute persuasive authority on the next appellate court confronting the Relationship Privacy Act. The state announced its plans to seek discretionary review with the Court of Criminal Appeals. However, regardless of what that court or other courts may ultimately decide, the well-reasoned opinion by Chief Justice James T. Worthen exposed fundamental flaws in the wording of the statute. If the Texas Legislature truly wants to protect its citizens from the evil of revenge porn, then it should go back to the drawing board and come up with a more artfully-worded statute that is content-neutral and sufficiently narrow in its focus so as to pass constitutional muster.

About the Author

John Browning is a shareholder in the Dallas, Texas firm of Passman & Jones, P.C., where he handles civil litigation in state and federal courts, in areas ranging from employment and intellectual property to commercial cases and defense of products liability, professional liability, media law, and general negligence matters. Mr. Browning has extensive trial, appellate, and summary judgment experience and has represented companies in a wide variety of industries throughout Texas. Mr. Browning received his Bachelor of Arts with general and departmental honors from Rutgers University in 1986, where he was a National Merit Scholar and member of Phi Beta Kappa. He received his Juris Doctor from the University of Texas School of Law in 1989. He is the author of the books *The Lawyer's Guide to Social Networking, Understanding Social Media's Impact on the Law*, (West 2010); the Social Media and Litigation Practice Guide (West 2014); Legal Ethics and Social Media: A Practitioner's Handbook (ABA Press 2017); and Cases & Materials on Social Media and the Law (forthcoming). Mr. Browning is also a contributing author to seven other books, the author of nearly 35 published law review articles; and the award-winning writer of numerous articles for regional and national legal publications. His work has been cited in nearly 350 law review articles, practice guides in 11 states, and by courts in Texas, California, Maryland, Tennessee, New York, Florida, Illinois, and Puerto Rico. He has been quoted as a leading authority on social media and the law by such publications as *The New York Times, The Wall Street Journal*, *USA Today, Law 360*, *Time* Magazine, *The National Law Journal*, the ABA Journal, *WIRED* Magazine and *Inside Counsel* Magazine, and he is a recurring legal commentator for the NBC, CBS, and FOX news stations in Dallas. He serves as Chair of the Texas Bar Journal Board of Editors, as a member of Professional Ethics Committee of the State Bar of Texas, and is a frequent speaker at CLE seminars and legal symposia all over the country. In March 2018 Mr. Browning won the Republican primary for the Fifth Court of Appeals (Place 11), and will be a candidate in the November 2018 general election.

State Breach Notification Laws begin adding Cybersecurity Obligations

By Seth Jaffe

United States lawmakers have yet to promulgate a comprehensive federal cybersecurity law aimed at setting a cyber-hygiene standard for the commercial sector. But a collation of recently enacted industry-specific laws (both federal and state), proposed bills, guidance documents, and cyber strategies yields a fair indication of where our nation is headed. Increasingly, states are modifying breach notification laws to add cybersecurity obligations. Colorado amended its law in April of this year, and Alabama, the 50th and final state to pass a breach notification law, included a number of security requirements.

Data breach notification laws, at their core, require controllers of data subjects' personally identifiable information to notify said data subjects in the event of a breach. In other words, if a company loses the sensitive information of its customers, whether through accidental disclosure or cyber theft, it must notify these customers and (depending on the state), provide information such as the nature of the breach, what the company is doing to rectify the issue, and/or the contact information for the FTC or credit bureaus.[1] California kicked off the trend back in 2002 and every state has since followed suit, but it is worth looking closely at Alabama's law to get a sense of where we may be headed from a cyber regulation standpoint.

The Alabama Data Breach Notification Act of 2018 includes the usual notification provisions mentioned above, but then it goes on to require entities doing business in the state to "implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security." Alabama is not the first to obligate reasonable security provisions in its breach notification law[2] (Colorado revised its law just two months after Alabama to add that language), but Alabama's law does attempt to define

---

1 Covered entity obligations may vary by state. Several law firms offer free online summaries of state breach notification laws. Search for "breach notification chart" on your favorite search engine.

2 *See* laws from Alabama, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Indiana, Maryland, Massachusetts, New Jersey, New Mexico, Nevada, Oregon, Rhode Island, Utah.

reasonable security measures,[3] and in doing so, it falls in line with other states that have recognized the same eight steps as setting the minimum standard for an acceptable data security program.[4]

Step 1: Conduct a Risk Assessment

As far back as at least the Graham-Leach-Bliley act in 1999, authorities recognized the difficulty in designing a comprehensive cyber program without first identifying assets, understanding vulnerabilities, and forecasting attack vectors. For this reason, cyber laws are beginning to require comprehensive risk assessments at periodic intervals.

Alabama's law requires "[i]dentification of internal and external risks of a breach of security."

Step 2: Implement an Information Security Program

Information acquired during the risk assessment feeds into an overarching information security program, which generally includes, as in Alabama's case, "[a]doption of appropriate information safeguards to address identified risks of a breach of security and assess the effectiveness of such safeguards."[5]

Step 3: Involve the Board of Directors in Cybersecurity Management

Without buy-in from senior management, companies may find themselves culturally constrained when it comes to cybersecurity. Board of Director involvement can usually be satisfied through implementation of a process to percolate relevant cybersecurity information

---

[3] Given the recent holding in *Federal Trade Commission Act. LabMD, Inc. v. Federal Trade Commission*, No. 16-16270 (11th Cir. June 6, 2018) (ruling as unenforceable for relying on an indeterminable standard an FTC order to maintain a comprehensive information security program), states mandating "reasonable security procedures and practices," but nothing more, may find themselves facing challenge in the courts. For a more in-depth analysis of the FTC's interpretation of reasonable data security practices under its Section 5 powers, see Pierre Grosdidier and Cassidy Daniels, *2015 FTC Guidelines for Data Security*, Circuits (Nov. 2016), available at http://texasbar.informz.net/texasbar/data/images/Sections/2016-2017/Computer%20&%20Technology/Circuits%20November%202016/2015%20FTC%20Guidelines%20for%20Data%20Security_Page%2016%20-%2022.pdf.

[4] Massachusetts' 201 CMR 17, passed in 2009, set the benchmark for state law data security standards, though many were seen in earlier industry-specific laws such as Graham-Leach-Bliley, HIPAA, the FTC Red Flags Rule. At least two other states, New York (the SHIELD ACT) and North Carolina, are considering revisions to their breach notification laws to impose similar requirements.

[5] Massachusetts' 201 CMR 17.03 includes "[d]eveloping security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises."

up to the Board, as well as push down decisions to the company. The Board should have the ability to digest the information, which can be difficult if no members are conversant in cybersecurity technology; many Boards charter a cybersecurity committee for this purpose.

Alabama's law requires "[k]eeping the management of the covered entity, including its board of directors, if any, appropriately informed of the overall status of its security measure."

Step 4: Designate an Individual in Charge of Cybersecurity

Often referred to as a Chief Information Security Officer ("CISO"), a company must designate an individual with the authority to oversee the security program and assume accountability should incidents occur.

Alabama's law requires "[d]esignation of an employee or employees to coordinate the covered entity's security measures to protect against a breach of security."[6]

Step 5: Maintain an Incident Response Program

Cyber professionals are quick to point out that organizations in the midst of an incident are notoriously terrible at improvising. The National Institute of Standards and Technology in its Computer Security Incident Handling Guide (800.61r2) refers to incident response as a "complex undertaking," necessitating "clear procedures for prioritizing and handling incidents." Without a comprehensive enterprise cyber crisis management plan, mistakes will be made.

Although Alabama does not reference incident response by name, it mandates that a covered entity "conduct[] a good faith and prompt investigation" in the event of a data breach.[7]

---

[6] Many cybersecurity laws having this principle allow for third party providers to staff this position. New York's Department of Financial Services Section 500.04, for example, allows the covered entity to satisfy the CISO requirement so long as it retains compliance responsibility, designates a senior manager to oversee the third party, and requires the third party to maintain a cybersecurity program.

[7] Cyber law trends appear to be settling on more defined incident response requirements, such as New York Department of Financial Services Section 500.16, which requires "a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event."

Principle 6: Manage Cybersecurity of Third-Party Vendors

Baker Hostetler's 2018 Data Security Incident Response Report[8] attributed 31% of successful network attacks to vendor wrongdoing, up from 15% the year before. Regulating authorities are taking note of this trend, as is evident from two recent settlements related to data breaches caused by a third-party.[9]

Alabama's act obligates "[r]etention of service providers, if any, that are contractually required to maintain appropriate safeguards for sensitive personally identifying information." It also paints a target on the third-party agent, subjecting it to Alabama's penalty provisions of up to $500,000 per breach.

Step 7: Conduct Routine Security Training

A company's cyber program is oftentimes only as robust as the employees implementing it. A number of statistics put insider threats as a leading cause of data breaches. Whether it is because employees invariably click on suspicious links in emails, use easily defeatable passwords, fail to report malicious or accidental cyber issues, or simply do not practice good cyber hygiene, poorly trained employees are often the weakest link in a cybersecurity program.

Alabama does not expressly mandate a training program in its Act, though it may be implied through safeguards necessary to address internal risks. Massachusetts' law provides for "ongoing employee (including temporary and contract employee) training."

Step 8: Regularly Update the Program

Authorities recognize that cybersecurity is a living program, requiring continuous modifications as new threats arise, infrastructure changes, and reorganizations occur. Companies are instructed to modify the program accordingly, but at the very least, it should be reviewed and updated annually.

The Alabama Act requires "[e]valuation and adjustment of security measures to account for changes in circumstances affecting the security of sensitive personally identifying information."

---

8 Available at http://e.bakerlaw.com/cv/1b9a4641d614c480ed4717b172941994eaf8dea5/p=8213342.

9 *See* Decision and Order, *In re BLU Products, Inc.*, FTC No. 1723025 (April 30, 2018); Plaintiff James Graham's Motion for Preliminary Approval of Derivative Litigation Settlement, *In re The Wendy's Company Shareholder Derivative Action*, No. 1:16-cv-01153 (S.D. Ohio May 6, 2018) (Pacer Doc. 41).

Conclusion

As lawmakers struggle to address the ever-increasing impacts of cybercrime, we can expect additional cybersecurity requirements designed to accelerate the collective defense of our economy and its varying industries.[10] At least fifteen states have already imposed "reasonable security measure" standards.[11] Deploying safeguards, controls, and processes included in the above eight steps may well put your clients ahead of the curve.[12]

---

[10] Ohio's new law, going into effect in November of 2018, provides safe harbor from tort cases for entities reasonably conforming to certain cyber security standards. *See Substitute Senate Bill No. 220*, 132 G.A. (Ohio 2018). This new law will be the topic of a subsequent article.

[11] *See* footnote 2, *supra.* The FTC maintains an informative website on data security, available at https://www.ftc.gov/datasecurity.

[12] Comprehensive cybersecurity programs may show a return on investment in the near future as customers look to cyber scorecards in selecting vendors.

Have You RSVP'd to Pro Bono Week?

By Hannah Allison, Pro Bono Programs Administrator

Texas is RSVP'ing YES to pro bono week this year. How about you?

Not sure what it is? The Celebrate Pro Bono homepage reads, "…this initiative provides an opportunity for legal organizations across the country to collaboratively commemorate the vitally important contributions of America's lawyers and to recruit and train the many additional volunteers required to meet the growing demand. With the enthusiastic involvement of national, statewide and local partners, from all components of the legal profession, the National Pro Bono Celebration is creating a wave of positive energy about the pro bono movement in this country..."

The year marks the 10th anniversary of National Pro Bono Week, October 22–26. ABA President Bob Carlson is encouraging organizations to plan and participate in events focused on **disaster resiliency**.

Disaster survivors face countless legal issues—from insurance disputes, FEMA appeals, landlord–tenant disputes, consumer fraud, health and education issues, and so much more. Even before a disaster strikes, communities need legal assistance with **disaster preparedness** through business continuity planning, securing title documents, meeting insurance needs, and other assistance. How can you get involved in October?

Online Pro Bono Clinic

Following the impact of Hurricane Harvey on the Texas coast, attorneys found an easy way to participate in pro bono by volunteering with Texas' new online legal advice clinic, Texas Legal Answers. It took just three minutes to sign up for www.TexasLegalAnswers.org, under *Volunteer Attorney Registration*, and within the first month following the disaster there were Harvey questions hitting the queue. To date, Texas Legal Answers has received 65 direct questions in the natural disaster category with hundreds more coming in that are indirect legal issues that arose following Harvey.

Client surveys are showing feedback like,

> **"This was a terrific way to get questions answered and it was obvious that whoever answered the question for me was both knowledgeable and compassionate. Thank you so much."**

With an average question taking just 20 minutes for an attorney to answer, you can easily log pro bono hours during pro bono week and empower Texans to receive access to justice anywhere you have internet access. Maybe while you wait for your Frappuccino? Or while you wait for your oil change?

Volunteer attorneys are also benefiting this program:

> **"I became an attorney to do good—and helping those that need help is a part of that. Texas Legal Answers is a quick and simple way to give back and help without turning away your attention from your existing caseload."**

For every question answered during pro bono week, volunteers will receive an entry to win a new Kindle Fire—generously donated by Westlaw—and a Pro Bono Texas swag bag. Can you #Give20Minutes?

Social Media

How about daily social media posts, covering the week of October 22–26? You could focus on how technology can assist in a disaster or ideas on technological preparedness for attorneys and their practice. Whether it is physical space considerations, network and phone backup ideas, or any statewide or national resources that are available to assist with technological needs following a fire, flood, etc., y'all have the resources and knowledge base—share it! Need a starting point for ideas? Check out the ABA's Committee on Disaster Response and Preparedness page here.

If not social media, how about writing a short blog post for the Texas Bar Blog? Again, focusing on the above topics and connecting it to national pro bono week.

Find an Event

Don't have enough time in the day to plan your kid's fall soccer schedule, let alone build something for pro bono week? Let someone else do the planning and you can simply show up for a pro bono week event near you. Watch over the coming weeks, as organizations add events to the National Pro Bono Week calendar.

Texas has your Back

Already doing pro bono, but looking for some resources to make it a tad easier? Need a mentor for a case that is outside your practice area? Maybe you haven't dipped your toe in pro bono, but now you are ready? Texas has your back with ProBonoTexas.org. It is a one-stop shop for all things pro bono—including ways to find new pro bono opportunities, a resource library to

help you find those answers for Texas Legal Answers, and Westlaw Doc & Form Builder to maximize your efforts when assembling documents for your pro bono clients.

Pro Bono Texas will be pushing out social media posts, giveaways, fun facts, etc. across pro bono week on Facebook and Twitter. Stay tuned for announcements and event highlights from across the state.

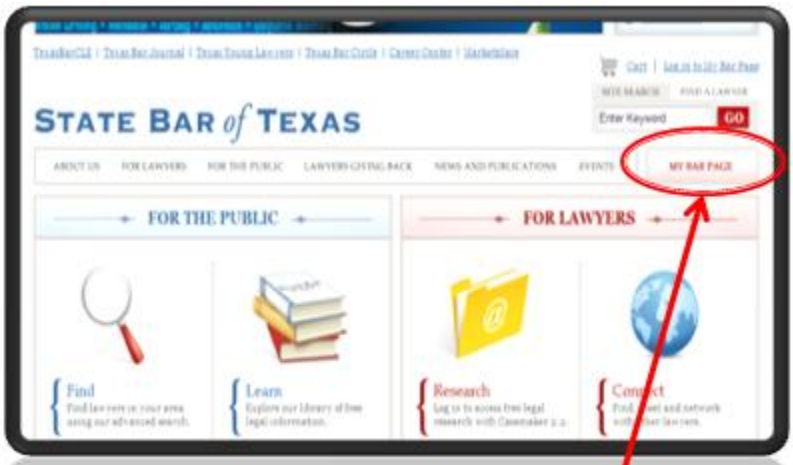
Do you know a pro bono rock star or are you yourself a pro bono enthusiast? Give us a shout here!

About the Author

Hannah Allison is the pro bono programs administrator for the Legal Access Division of the State Bar of Texas and manages Texas Legal Answers. If you have questions or would like to chat about all things pro bono, you may contact her at probonotx@texasbar.com.

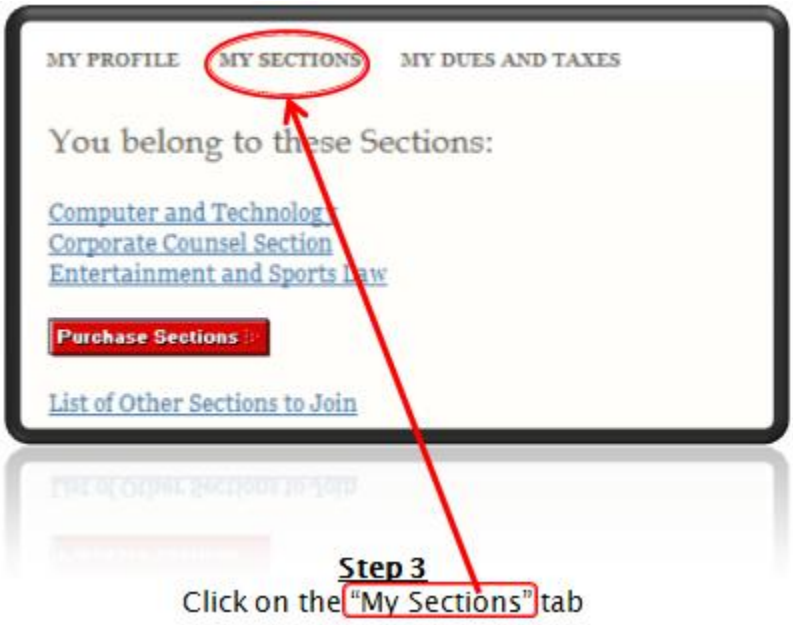
How to Join the State Bar of Texas Computer & Technology Section

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

Sammy Ford IV – Houston – Chair
John Browning – Dallas – Chair-Elect
Shawn Tuma, Fort Worth – Treasurer
Elizabeth Rogers – Austin – Secretary
Michael Curran – Austin – Past Chair

Webmaster

Pierre Grosdidier – Houston

Circuits Co-Editors

Pierre Grosdidier – Houston
Kristen Knauf – Dallas/Fort Worth

Term Expiring 2021

Chris Krupa Downs – Plano
Seth Jaffe – Houston
Honorable Emily Miskel – Collin County
William Smith – Austin

Term Expiring 2020

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

Term Expiring 2019

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

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