15 Cases and Statutes in 45 Minutes

By Lisa Angelo, Pierre Grosdidier, Shawn Tuma

(This article will be presented at a speakers’ panel at the June 2019 Texas Bar Conference in Austin, Texas.)

This article briefly summarizes 15 recent cases, statutes, and legal developments that every Texas attorney should know about.

1. Business Duty to Protect Sensitive – Personal Information & Notify of Breach
The Texas Identity Theft Enforcement and Protection Act1 (ITEPA) requires those engaging in business in Texas (including lawyers and law firms) have cybersecurity and data privacy duties to: (1) implement and maintain reasonable procedures to protect electronic sensitive personal information (“SPI”) they collect or maintain;2 (2) follow appropriate data destruction procedures;3 and, (3) notify any individual whose SPI was or is reasonably believed to have been acquired by an unauthorized person.4

As of this writing, the 2019 Texas Legislature has passed (and it is believed the Governor will sign into law) HB 4390. HB 4390 amends the breach notification law with two major changes: (1) instead of “as quickly as possible,” notification now must be made “without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred;” and, (2) a person required to notify 250 or more residents of Texas must also notify the attorney general and provide five specific categories of information.

2. Texas Lawyers’ Competence in Technology
The Texas Disciplinary Rules of Professional Conduct were amended in early 2019, expanding a lawyer’s duty to maintain competence to include understanding the benefits and risks associated with relevant technology.5 This amendment follows the trend set by the American Bar Association after it issued a similar amendment to the Model Rules in 2018.6 Since 2017, the ABA has also issued opinions on lawyers’ obligations to protect client data and the proper

---

5 Tex. Disciplinary Rules Prof’l Conduct R. 1.01, Cmt. 8.
6 MODEL RULES OF PROF’L CONDUCT R. 1.1, Cmt. 8 (2018).
steps to respond to a data breach. The opinions reiterate how rules of ethics apply in the digital era.

3. **Digital Border Searches**

Digital border searches of laptops, tablets, and smart phones (both inbound and outbound) are legal. The key issues are (1) the distinction between basic and forensic searches; and (2) the level of suspicion required for each. No level of suspicion is required for basic searches, which means that authorities can rummage through your devices if they want. Circuit Courts are split regarding forensic searches, some requiring some suspicion, others none. The key cases are: *U.S. v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018); *U.S. v. Cotterman*, 709 F.3d 952 (9th Cir. 2013); and *U.S. v. Touset*, 890 F.3d 1227 (11th Cir. 2018). Separately, Custom and Border Protection (“CBP”) issued its revised digital search policy in January 2018 (CBP Directive No. 3340-049A, Jan. 4, 2018, available online). The policy recognizes that CBP may perform basic searches without suspicion. Forensic searches require suspicion and supervision. A special procedure applies to privileged information. For additional information, see Pierre Grosdidier’s article in the September 2018 *Circuits*.

4. **Consequences of Improper Data Destruction**

ITEPA requires Texas business to follow appropriate data destruction procedures and they will face consequences when they fail to do so. The Texas Attorney General has pursued claims against businesses for improperly disposing of documents containing SPI. One such case resulted in a $1,240,000 settlement for disposing of 3,000 medical records in a publicly accessible dumpster. Another case in 2015 also resulted in a settlement for disposing of documents containing SPI in a publicly accessible dumpster.

---

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf


5. **Consequences of Inadequate Security**

The Federal Trade Commission (“FTC”) complained that Uber Technologies, Inc. made misrepresentations about data security and engaged in unfair practices by failing to provide reasonable security to prevent unauthorized access to personal information.\(^{11}\) In its complaint, the FTC described a few of the practices it considered unreasonable to protect data such as Uber’s alleged failures to require multi-factor authentication and encryption. The FTC complained that based on the unreasonable security controls in place, Uber’s statements about data security were misrepresentations.

6. **Cell Phone Tracking Without Warrant**

In *Sims v. State*, the Texas Court of Criminal Appeals (“TCCA”) unanimously held that authorities did not violate a suspect’s Fourth Amendment privacy rights when they “pinged” his cell phone less than five times over less than three hours without a warrant to locate and arrest him on suspicion of murder.\(^ {12}\) The decision is consistent with *Carpenter v. United States*, where the U.S. Supreme Court recently held that a warrant was required to access seven days of cell-site location information (CSLI).\(^ {13}\) *Carpenter* was a narrow decision that left room for warrantless requests for CSLI under exigent circumstances, such as when authorities “need to pursue a fleeing suspect, [or] protect individuals who are threatened with imminent harm.”\(^ {14}\) For additional information, see Pierre Grosdidier’s *Feature Article* in the March 2019 Circuits.

7. **Lawyers’ Duties to Protect Client Data: Even Paper Files in a Stolen Vehicle?**

In recent years the discussion of lawyers’ duty to protect client data has focused on digital data, however, those same duties apply to protecting client data in traditional paper form. This issue is front and center in one recent case. MoneyGram hired Mark Kovalchuk to collect old debts from numerous individuals. MoneyGram provided its files to Kovalchuk, which included information about the debts owed and the debtors’ credit information. According to the allegations in the lawsuit, Kovalchuk then traveled from Minnesota to Arizona with the hard copies of the files and, along the way, “left boxes of documents containing confidential and/or personally identifiable information in Mr. Kovalchuk’s ‘tricked out Hummer H2’ while it was parked overnight at a hotel in Albuquerque, New Mexico—even though defendants chose to protect and to safeguard other items, such as their laptop and liquor, by bringing these items into their hotel room.” The “tricked out Hummer H2 was stolen from the Hyatt Place Hotel,

---

\(^ {13}\) 138 S. Ct. 2206, 2217 n.3 (2018).
\(^ {14}\) *Id.* at 2220, 22–23 (“Our decision today is a narrow one.”).
Uptown Albuquerque” and, along with it, the MoneyGram client files containing sensitive personal information of the debtors from whom MoneyGram was trying to collect its debts—individuals that MoneyGram would consequently be required to notify of this data breach. MoneyGram is suing Kovalchuk for gross negligence, among other things.\(^\text{15}\)

8. **Consequences of Inadequate Security Of Third Parties**

Shortly after learning its third-party vendor had unnecessary access to data, BLU Products, Inc. issued a statement claiming to have stopped the vendor’s unexpected access. However, the FTC believed otherwise and filed a complaint against BLU for misrepresenting that the vendor’s access had been restricted.\(^\text{16}\) The FTC also complained that BLU engaged in unfair practices by failing to implement appropriate cybersecurity procedures to oversee the security practices of third-party vendors.

9. **Shore v. Johnson & Bell, 16–CV–04363 (N.D. Ill., Apr. 15, 2016).**

A client initiated a class action against a law firm for its inadequate data security measures. The plaintiffs alleged that the law firm was “a data breach waiting to happen.” There was no actual harm and the case move to confidential arbitration, but not before the plaintiffs had made their point.

10. **Departing Lawyers and Outlook .pst Files**

The facts of this hypothetical situation are intended to help lawyers think about the issues that arise in a situation that happens in law firms every single day: A lawyer decides to leave a law firm and, in preparing to do so, copies to a USB thumb drive his Outlook .pst file that contains all of the emails the lawyer has sent and received on behalf of all clients for whom he has worked while at the law firm. The lawyer then takes the USB thumb drive full of the law firm’s client data, saves its contents in its entirety to the network of his new employer, and then loses the thumb drive. Who is responsible for the data on the USB drive? Who is responsible for securing the data on the USB drive? Who is responsible for notifying the entities and individuals that their sensitive information has been lost? Who has ethical obligations to keep confidential the data on the USB drive?


11. **Consequences of Inadequate Security of a Sole Proprietorship**

A sole proprietor’s claims ensuring security of users’ account information by using the latest encryption and security techniques were misleading, according to the FTC’s complaint. The FTC also complained that the sole proprietor was engaged in unfair practices based on its unreasonable data security.

12. **Consumer Data Protection Act**

Senator Ron Wyden (D–OR) introduced S.2188, a bill entitled the “Consumer Data Protection Act” (CDPA). The proposed statute is the first federal foray into consumer privacy laws. The CDPA applies to “covered entities,” which are defined as entities that have $50 million or more in annual revenue and that have records for a million or more consumers. The Act would, inter alia, define “personal information” very broadly, grant the FTC oversight authority in the domain of consumer personal information, and require the FTC to deploy a “Do Not Track” website that would allow consumers to “opt-out” of data sharing. For additional information, see Pierre Grosdidier’s *ShortCircuit* in the December 2018 *Circuits*.

13. **Contractual Exclusion in Cyber Insurance**

When procuring cyber insurance, it is important for companies to know if the insurance will cover claims that are contractual in nature, such as routine indemnity agreements contained in many contracts. Some policies have language excluding contractual liability, such as an exclusion for “actual or alleged liability under a written or oral contract or agreement.”

This exclusion was the focus of a recent case between Spec’s Family Partners and its insurance carrier. Spec’s had previously had a breach of payment card data and, pursuant to its contract with its merchant bank that processed its payment cards, Spec’s was required to pay fines to the merchant bank. The merchant bank sued Spec’s and Spec’s made a claim for defense on its insurance policy. The claim was denied because, among other things, it was based on a contractual obligation by Spec’s to pay its merchant bank. The case ultimately made its way to the Fifth Circuit, which found that, because there were claims that were not contractual in nature (negligence), there was a duty to defend that was triggered.

---


14. **Cyber Insurance Dispute**

According to its complaint, Mondelez International, Inc. was one of many victims of a ransomware attack known as NotPetya. Mondelez submitted an insurance claim to its carrier, Zurich American Insurance, which was subsequently denied based on a policy exclusion. Mondelez filed suit against Zurich, claiming that the insurance claim was improperly denied. Even though this lawsuit is currently pending, the complaint highlights important considerations for insureds hoping to have coverage for similar cyber threats.

15. **LabMD v. FTC, 894 F.3d 1221 (11th Cir. 2018)**

After more than a decade of litigation, the Eleventh Circuit brought the FTC’s case against LabMD to an end. The FTC had taken LabMD, a medical testing company, to task for its lax data security measures. The case resulted in a lengthy and controversial decade of litigation that involved a congressional inquiry and a criminal investigation. The ALJ initially dismissed the FTC’s case against LabMD but the full commission reversed, ordering the company to overhaul its security measures. By then, LabMD had ceased all operations for years. The Eleventh Circuit held that “the Commission’s cease and desist order is nonetheless unenforceable. It does not enjoin a specific act or practice. Instead, it mandates a complete overhaul of LabMD’s data-security program and says precious little about how this is to be accomplished. Moreover, it effectually charges the district court with managing the overhaul. This is a scheme Congress could not have envisioned. We therefore grant LabMD’s petition for review and vacate the Commission’s order.” For additional information, see Jamie Sorley’s Feature Article in the December 2018 *Circuits*.

---

**About the Authors**

Lisa M. Angelo is a cyber liability attorney and Certified Information Privacy Manager. Her law practice is focused on advising clients on data privacy, cyber insurance, technology contracts, and other matters related to cyber and technology law.

---

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 and unauthorized computer access 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, a registered P.E. in Texas (inactive), and the State Bar of Texas Computer & Technology Section Webmaster and Circuits eJournal Co–Editor for 2018–19.

Shawn Tuma is an attorney internationally recognized in cybersecurity and data privacy law, which he has practiced for 20 years. He is a Partner at Spencer Fane LLP. In 2016, the National Law Journal selected him as a Cybersecurity Law Trailblazer and Texas SuperLawyers selected him for the Top 100 Lawyers in DFW.