Contents

Message from the Chair

By Shannon Warren

Where do the intersection of technology and law meet?

For many lawyers, technology is a mere tool to be used for typing up pleadings or communicating with others. Others have enjoyed the smartphones, tablets, and apps which have been released in the last decade. Indeed, the networks and computers you and I carry around today are a small reminder of how far we have come. That "gee-wiz" tool is great for capturing images, connecting with old friends, sharing a thought or ordering a cup of coffee at the nearest coffee house.

What if you were told that the relative conveniences of the smartphone and social networks were nothing compared to what is about to occur in the world of computers and technology?

Arthur C. Clarke formulated three prediction-related adages, the third of which is most famous:

> "Any sufficiently advanced technology is indistinguishable from magic."

We are alive in a time of magic. The computer systems and software of our time are becoming so smart, so connected, and so cheap to operate that we are on the precipice of a new computing era.

Maybe you have already noticed the changes. Virtual Personal Assistance such as Siri, Cortana and Google Assistant is getting smarter and more conversational. Large retailers such as Target and Amazon are anticipating our purchases and providing coupons before we know we needed something. Sports scores and articles are no longer written by humans, but A.I. driven algorithms, designed to construct game summaries for sports fans. Movie and music recommendations by Spotify, Netflix and Pandora are curated by software, not humans. Even customer service is getting smarter with chat bots that pretend to be human but are A.I. systems.

If this all sounds cute and interesting, then do not get too comfortable. A.I. is coming for our industry too.

Major platform companies, such as IBM, are already selling A.I. as a service. Meaning, developers can hire the IBM systems and, effectively, plug it into their software.

Soon, firms can use A.I. based software to read through tens of thousands of pages of material, understand the contents, and make reasoned arguments based on the source material. This is already happening in medicine and early software services for law look very promising.

What does this mean for you, a lawyer in the early twenty-first century? Does this mean that you are about to be replaced by a robot?

We believe that the role of a lawyer as counselor, mentor and advocate cannot be delegated to computer systems. In computer terms, you are the "interface" between the client and the law. However, you must be prepared to use the new systems to keep up with the state of the law, and the benefits of the A.I. systems of our time.

So, the answer to the question "Where do the intersection of technology and law meet?" will increasingly be the well-equipped lawyer. Lawyers will be responsible for considering the quality of the tools as they come to market and providing value to clients in an age where online platforms promise to replace you.

That's where we come in.

The Computer and Technology Section is committed to helping its members and the Bar in general to be prepared for the coming era. Our mission is to educate and involve the legal profession in and about the use and law of computer and information technology.

As we work to educate and equip our members, our focus areas are (1) new tools and tech gadgets, (2) eDiscovery, (3) privacy, (4) cybersecurity and computer abuse, (5) social media and the law, (6) legal ethics related to technology, and (7) artificial intelligence and the law. Please join us as we seek to educate one another in these topic areas.

Letter from the Editors

By Elizabeth Rogers and Antony P. Ng

A new bar year had begun since the previous edition of *Circuits*, and our former editor Michael Curran is now the Chair Elect of the Computer & Technology section. We wish Michael the best in his new position, and we will continue to strive to provide you the bleeding edge of knowledge in the intersection of law and technology.

In the current edition, John Browning explores the risk of inadvertent confessions in world of social media, and Nick Sarokhanian follows up with the various evidentiary issues of using those information in court. As the concept of data security has been slowly making its way to many lawyers' cerebral cortex, Pierre Grosdidier and Cassidy Daniels treat us with an overview of the data security guidelines promulgated by the Federal Trade Commission.

When some of you suggested a tech tip segment, we here at *Circuits* listened. For the first time, we have provided a list of keyboard shortcuts that are commonly used in legal documents in Word format.

We hope that you enjoy the content of the current edition, and we encourage you to submit feedback and suggestions to Elizabeth Rogers at rogersel@gtlaw.com or Antony P. Ng at ng@russellnglaw.com.

The Dangers of the Digital Confessional

By John G. Browning

In his book Exposed: Desire and Disobedience in the Digital Age, legal and political theorist Bernard Harcourt posits the theory that with the advent of social media, humans are forsaking our broader freedoms for the sake of small doses of social interaction that give us pleasure. A generation raised on reality TV now yearns to be "internet famous" as we trade privacy for Facebook likes and shares, retweets, and other illusory connections. We live in what Harcourt calls an "expository society", where privacy is no longer a core value and "all the formerly coercive surveillance technology is now woven into the very fabric of our pleasure and fantasies." We want to expose ourselves and to see others exposed, we want to see and be seen, and to reinvent ourselves online. For lawyers however, there are real world consequences to this shift in societal attitude in which digital intimacy is becoming the new norm. In a world in which 75% of the adult population maintains at least one social networking profile, and in which 293,000 status updates are posted on Facebook every minute and roughly a billion tweets are processed every 48 hours, people are providing the very ammunition that lawyers will use to impeach their claims or defenses and impugn their credibility. Moreover, as a growing number of state ethics opinions call for attorneys to be aware of what their clients are posting on social media and take an active role in advising what to take down (or not post in the first place), it's become more important than ever for lawyers to serve as a kind of digital "client's keeper".[1]

Consider, for example, the potential impact on cases where the lawyer is unaware of such postings. In a recent Florida employment discrimination case, Gulliver Schools, Inc. v. Snay, the former headmaster of a private academy sued for discrimination.[2] The case resulted in a $150,000 settlement ($70,000 of which was attorney's fees and back wages) which contained a standard confidentiality provision calling for any settlement monies paid to be forfeited if the plaintiff disclosed the account or terms of the settlement to any third parties. When the defendants learned of a Facebook post by the settling plaintiff's daughter that breached this confidentiality clause (it read "Mama and Papa Snay won the case against Gulliver. Gulliver is

---

[1] See, for example, John Browning and Al Harrison, "What is THAT Doing on Facebook?! A Guide to Advising Clients to 'Clean Up' Their Social Media Profiles," 53 Houston Lawyer No. 4 (Jan/Feb. 2016); John Browning, "A Clean Slate or a Trip to the Disciplinary Board? Ethical Consideration in Advising Clients to 'Clean Up' Their Social Media Profiles," 48 Creighton Law Review No. 4 (September 2015)

[2] 2014 WL 769030 (Fla. Dist. Ct. App. 2014)

now officially paying for my vacation to Europe this summer. SUCK IT."), they sued. The court had no problem finding that the disclosure by Snay to his teenage daughter leading to the Facebook post was a breach of the settlement agreement; it ordered a disgorgement of Snay's $80,000 settlement. In West Virginia, Kanawha County public defender Sara Whitaker found herself before a judge accused of contempt in December 2015 after allegedly giving her client a copy of a packet containing the identity of a confidential informant.[3] The informant's name and address were posted on Facebook by the former roommate of client Tracie Jones, complete with captions like, "exposed" and "cheap whore". Although Whitaker ultimately received only a fine, this case illustrates how quickly a client's social media posts could lead to witness intimidation charges as well as potential ethical violations for the lawyer.

Another cautionary tale about the importance of monitoring a client's social media activities comes straight from the headlines. Famed rapper 50 Cent filed for bankruptcy in 2015 in the wake of a $7 million jury verdict against him. But evidently, 50 Cent (real name: Curtis Jackson, III) didn't quite grasp the underlying concept of Chapter 11 bankruptcy, because he proceeded to post numerous photos to his social media accounts, including Instagram, depicting him holding, pointing to, or surrounded by stacks and stacks of cash. One photo showed stacks of cash stashed in his refrigerator. Another featured the rapper with money strewn across his bed (along with a caption referencing 50 Cent's song "I'm Too Rich"); and yet another showed the singer with stacks of cash carefully arranged to spell the word "BROKE".[4] His creditors, including headphone company Sleek Audio and SunTrust Bank were not amused and filed pleadings bringing the photos to the court's attention, and implying that 50 Cent was hiding assets. The rapper's lawyers insisted that the photos were being publicized in an attempt to "smear" 50 Cent, said that his social media postings were simply part of maintaining "his brand and image," and even maintained that the stacks of cash were from a Hollywood prop company and were not actual currency. Concerned about "allegations of nondisclosure and a lack of transparency in the case," Connecticut bankruptcy judge Ann Nevin ordered 50 Cent to appear and explain the photographs at a hearing. Despite the gravity of his situation, 50 Cent continued to post on Twitter and Instagram, including one photo depicting the rapper with stacks of cash stuck in his waistband that was apparently taken inside the federal courthouse in Hartford. Judge Nevin was clearly not amused and scolded the rapper saying "There's

---

[3] Erin Beck, "Lawyer Will Have to Explain Informant ID Release," West Virginia Gazette (Dec. 17, 2015)

[4] Katy Stech, "Bankruptcy Judge Scolds Fifty Cent for Courthouse Photo," Wall Street Journal (April 7, 2016)

nothing funny going on here. This is very serious stuff." Ultimately, though, the court stopped short of banning him from posting to social media accounts.[5]

Yet even when clients aren't posting on social media during pending legal proceedings, all too frequently individuals are providing the very evidence against them in the form of social media – despite an acute awareness of their wrongdoing. The compulsion to share everything has resulted in social media serving as a kind of "digital confessional," in which people confess, flaunt, or otherwise share their transgressions with an online audience of potentially millions, Fifth Amendment right against self-incrimination flying out the window. Even as they themselves control the narrative, they destroy any chance at innocence as they fulfill Harcourt's predictions of an expository society. Consider the case of 22 year-old Matthew Cordle, who on September 3, 2013 uploaded a 3 ½ minute long video to YouTube that chillingly stated, "My name is Matthew Cordle, and on June 22, 2013 I hit and killed Vincent Canzani. This video will act as my confession."[6] Cordle had driven drunk that day in June and following the accident was found to have a .19 blood alcohol level. Within days of posting the haunting confession, Cordle's video had gone viral with over 1.3 million people viewing it. Ultimately, Cordle pled guilty to aggravated vehicular homicide and received a 6 ½ year sentence. While Cordle insists that he wanted to send a message about the dangers of drunk driving, cynical commenters speculated that the YouTube confession was a ploy done with the hope of a lenient sentence.

Good intentions were presumably absent when 16 year-old Maxwell Morton and 33 year-old Derek Medina posted their respective crimes. In 2015, Morton shot his friend and classmate Ryan Mangan in the face, and then posed with the corpse for a grisly selfie posted to Snapchat. He sent it to another friend (including the caption "Ryan was not the last one") who captured a screenshot before it disappeared and showed it to his mother, who alerted authorities.[7] The Pennsylvania teenage ultimately confessed and was charged as an adult with first degree murder. Similarly, in Florida Derek Medina killed his wife Jennifer Alonso at their house, took a photo of the dead body, and uploaded it to Facebook with the status update "I'm going to

---

[5] Id.

[6] Christine Ng, "YouTube Drunk Driving Confession Sentenced to 6.5 Years Despite Daughter's Plea for Maximum," ABCNews.com (Oct. 23, 2013)

[7] http://www.foxnews.com/us/2015/02/07/pa-cops-say-teen-killed-another-teen-posed-with-body-for-selfie.html

prison or death sentence for killing my wife."[8] True to his Facebook prediction, in 2016 Medina was convicted of second-degree murder and sentenced to life in prison.

With new technologies, individuals have found new ways to share their wrongdoing. Live streaming apps like Periscope, Meerkat, Twitch, and Facebook Live host untold hours of footage that provide a glimpse into users' personal lives for sharing with potentially huge audiences. On Periscope alone people are viewing the equivalent of 40 years worth of live videos every single day. Snapchat introduced its "Live Stories" feature in 2015, and it already has 100 million daily active users with 8 billion video views each day. Facebook CEO Mark Zuckerberg has touted the visceral appeal of live streaming apps. Because it's live, there is no way it can be curated. And because of that it frees people up to be themselves. It's live; it can't possibly be perfectly planned out ahead of time."[8a]

Using Periscope, people have live streamed their own drunk driving offenses, committing DWIs while a live audience – including law enforcement – watched and commented. In March 2016, 33 year-old Ahmed Almalki of Long Island, New York live streamed his drunk driving. State police received multiple calls about Almalki's driving from Periscope viewers and logged in themselves. Identifying his surroundings from the live streaming, they caught up with him and charged him with felony DWI.[9] Similarly, in October 2015 24 year-old Whitney Beall of Lakeland, Florida live streamed her drunk driving on Periscope. Footage shows Beall driving through neighborhoods, hitting a curb and flattening a tire on her Toyota Corolla, describing herself as "drunk beyond belief" and slurringly expressing her hope that she doesn't get a DWI because it would hurt her chances of getting into a neurology department.[10] A number of texts were sent to Beall's cellphone from people pleading with her to stop driving before she killed herself or someone else, and commenters posted throughout the live video, asking "how is she still driving?" Others alerted the police, who finally stopped her. While Periscope videos stay on the site for only 24 hours, a detective was able to capture and preserve the video as evidence. In February 2016, Beall pleaded no contest and received a standard sentence for a first-time offender; however, she also received an enhanced sentence (150 hours of

---

[8] http://cbsnews.com/news/florida-facebook-killer-derek-medina-who-killed-his-wife-posted-photo-sentenced

[8a] Rossalyn Warren, "When Rape is Broadcast Live on the Internet", www.buzzfeed.com (April 20, 2016)

[9] Patrick Lohmann, "Long Island Man Live Streamed His Drunk Driving State Police Say," www.syracuse.com (March 14, 2016)

[10] John Chambliss, "Lakeland Woman Who Went Live While DUI Sentenced," www.ledger.com (Feb. 17, 2016)

community service and 10 days of weekend work release) for "publicly flaunting her disregard for the safety of the community." And in another episode that could have ended tragically, two Sacramento men Periscoped their armed hunt for another individual suspected of sleeping with one man's girlfriend.[11] 28 year-old Damon Batson and 25 year old Carlos Gonzalez live streamed their search, at one point responding to a viewer who asked if their gun was real by firing it. Other viewers egged the men on, "liking" the broadcast with heart emogis and comments. Police found out about the episode, viewed a recording and arrested Batson and Gonzalez after identifying them from the video.

In one of the most disturbing cases yet, 29 year-old Raymond Gates and 18 year-old Marina Lonina were charged in the alleged rape of an intoxicated 17 year-old girl in February 2016 in Columbus, Ohio. What makes this case so unusual is that Lonina – a supposed friend of the victim – was in the room at the time and live-streamed the alleged assault using Periscope to an online audience.[12] Lonina is depicted pulling on the victim's leg, and the girl can be seen struggling, screaming "no, it hurts so much," and "please stop" while Lonina giggles and laughs, according to prosecutors. Police were notified of the alleged attack not by Periscope's monitoring team, but by a friend of Lonina's watching the live stream from another state. Both Gates and Lonina have been charged with kidnapping, rape, sexual battery and pandering sexual matter involving a minor. Lonina's lawyer claims his client made "substantial" efforts to thwart the assault and maintains that Lonina was "swept up by the gravity of the situation" and "was filming in order to preserve" evidence, "not to embarrass or to shame or to titillate anybody." Understandably, Franklin County prosecutor Ron O'Brien has a very different viewpoint. Noting that "I have never seen a case such as this where you would actually live-stream a sexual assault," O'Brien believes that Lonina was enthralled by positive feedback online and that she "got caught up in the likes."[13]

Certainly, the live streaming of such criminal activity raises a whole host of legal issues, including what obligations companies like Periscope might have regarding the monitoring and removal of such content (Periscope, it should be noted, has rules banning pornographic and overtly sexual content, as well as explicitly graphic content or media intended to incite violent, illegal, or dangerous activities). Could a viewer of one of the live streams be called as a witness

---

[11] "Police: Men Hunted Victim in Midtown Sacramento on Periscope," CBS13-Sacramento (Aug. 28, 2015)

[12] Mike McPhate, "Teenager is Accused of Live-Streaming A Friend's Rape on Periscope," The New York Times (April 18, 2016)

[13] Id.

in court to testify to what he or she observed? If someone "likes" such activity, or live streams criminal behavior in public would he or she be subject to prosecution as an accessory?

Another tragic and recent case raises other questions about society and digital confessionals. In May, 2016, a 19 year-old French woman live-streamed her own suicide on Periscope. She engaged with viewers in a series of videos, promising a live stream of "importance" and stating "The video I am doing right now is not made to create buzz, but rather to make people react, to open minds, and that's it."[14] Having previously sent a text message to a friend in which she accuses an ex-boyfriend of rape and abuse, the young woman then proceeded to jump in front of oncoming train at a suburban Paris railway station. The suicide happened live before around 1,000 viewers. Although the footage is no longer available on Periscope, excerpts from the videos – with the suicide blacked out – have been widely circulated on YouTube.

Criminal activities and suicide are not the only things that people are choosing to share with an online audience. The urge to share every moment with an encouraging, if unseen, group of people can lead to civil implications too. For example, the plaintiff in a recent auto accident case filed in April in Spalding County, Georgia blamed not only the teenaged driver who collided with him, but Snapchat as well.[15] In particular, the lawsuit holds Snapchat's "speed filter," a feature that tracks the speed of its users, responsible for the crash. The speed filter uses a phone's GPS system to calculate the speed at which a user is moving at the time the "snap" (the photo or short video that can be edited to include filters, effects, text, captions and even drawings) is created. The speed reading is then added to the photo or video from the editing screen with a simple swipe to the left. According to the complaint filed by the plaintiffs Wentworth and Karen Maynard, on September 10, 2015 18 year-old Christal McGee was using Snapchat while driving her Mercedes. It alleges that she was motivated to drive fast – in this instance 113 mph – due to the Snapchat speed filter, and that Snapchat incentivized users of different features of its app by giving "trophies," making it "more of a game." The suit maintains that one of the three passengers in McGee's vehicle urged her to slow down but that she refused, arguing that she was "just trying to get the car to 100 miles per hour to post it on Snapchat." McGee supposed said, "I'm about to post it.", when the impact with Maynard's car occurred. While this case is in the early stages, there may be some merit to the claim of

---

[14] Lilia Blaise and Benoit Morenne "Suicide on Periscope Prompts French Officials to Open Inquiry," The New York Times (May 11, 2016)

[15] Debra Cassens Weiss, "Suit Blames Snapchat's speed tracker for high-speed auto accident," ABA Journal (April 28, 2016)

Ms. McGee's social media obsession the teen took a selfie of herself on a stretcher after the accident and posted it to Snapchat with the caption, "Lucky to Be Alive." McGee had allegedly been driving home from work at a local restaurant with three co-workers. Plaintiffs' counsel justifies suing Snapchat on product liability grounds, while Snapchat points out that its app includes a warning that it shouldn't be used while driving.

If the allegations in Maynard's case are correct, it adds another dimension to our notion of a digital confessional. Users of social media are sharing everything, including the most heinous of criminal acts, driven to sacrifice privacy by an overwhelming need for attention and reinforcement in the form of "likes", shares, and retweets. The risk of self-incrimination and civil liability, it would seem, takes a backseat to the fleeting, transient illusion of digital intimacy. As lawyers, we may be called upon to exploit it or defend against it, but first we must be aware of this trend.

About the Author:

John G. Browning is a shareholder in the Dallas law firm of Passman & Jones, P.C, where he practices a wide variety of civil litigation in state and federal courts. He is the author of three books and numerous articles on social media and the law, and he serves as an adjunct professor at SMU Dedman School of Law and at Texas Tech University School of Law. Mr. Browning's work has been cited by courts across the country and in numerous law review articles, and publications like The New York Times, TIME magazine, Law 360, and others have quoted him as a leading expert on social media and the law.

Using Out of Court "Tweets" at Trial

By Nicholas A.F. Sarokhanian

In a breach of loyalty, Jones ditched your company, pilfered crucial information and staff, and started his own competing venture. Unsurprisingly, you have to prove Jones' bad conduct circumstantially. Thankfully, you were able to capture some Twitter "tweets" (Twitter is a social media platform where users post messages of up to 140 characters to their "followers," which may be total strangers to the user) from Jones and his co-conspirators to fill in the gaps left by Jones' paltry production. But how do you use tweets to tell the story of Jones' betrayal to the jury on cross-examination? Many articles explain how to *authenticate* tweets; this article is designed to help you clear the hearsay hurdle your opposing counsel will surely throw in your path.

First Things First: What is Hearsay?

Hearsay is an out of court statement of a declarant that is offered for the truth of the matter asserted. *See* Tex. R. Evid. 801, 802; Fed. R. Evid. 801(c), 802. Many out of court statements are not hearsay at all, e.g., admissions of a party opponent; are not offered for the truth of the matter asserted but to establish some other fact; or are admissible as an exception to the hearsay rule. *See, e.g.*, Tex. R. Evid. 803(3) (present sense impression); Fed. R. Evid. 803(3) (same).

The best strategy is to get a ruling that the social media is not hearsay at all, and, if necessary, work your way through the applicable exceptions to the hearsay rule.

Not Hearsay: Tweets as Admissions of Party Opponent

In Texas, there are five types of statements that are considered non-hearsay admissions of party opponents. *See* Tex. R. Evid. 801(e)(2)(A)-(E); Fed. R. Evid. 801(d)(2). For the sake of brevity, let's look at two common types of these admissions.

The first example is the easiest. Say Jones tweeted the following tweet while he was still employed by your client and while he was stealing your client's pricing strategies:

Use this tweet to show that Jones planned to compete with your client. This is Jones' own statement and should be admitted as an admission of a party opponent.

The second example is a statement made by Jones' co-conspirators. Smith and Johnson quit within days of Jones leaving. On Jones' last day, he made a tweet that "mentioned" Smith and Johnson (the @ symbol preceding a name is a way to include another user in one's tweet) and used a "hashtag" (the # sign) in an expressive manner:

Use this tweet as foundation that Smith and Johnson were with Jones celebrating his last day, that #teamwork indicates that they were working with Jones on something, and that #OnToTheNextOne tends to show they were working with him on his new company instead of benignly working together for your client. This should be admitted (at least conditionally) to help you introduce Johnson's bombshell tweet to your best customer about being able to offer lower prices than your client can:

You can use this tweet when you tell the jury that your client lost MidWestRegionCustomer days after Jones and Johnson left, which tends to fill in the "gap" in the document production, undercut the defendants' argument that the loss of that customer was not proximately caused by their departure, and tends to prove up your client's damages.

An Exception: Present Sense Impression

Don't lose hope if a tweet is considered hearsay. Many courts are applying the "present sense impression" exception to the hearsay rule to social media. *See* Tex. R. Evid. 803(1); Fed. R. Evid. 803(1). This makes sense because social media is electronic, meaning it never really disappears like an oral statement might in a witness' memory (all tweets are archived at the Library of Congress), and thus tends to be more reliable than not. Moreover, because almost everyone carries a smartphone, and because social media encourages people to contemporaneously "share" even mundane parts of life immediately, there is a good chance tweets were made while or soon after the user perceived a statement (an example is a reporter "live-tweeting" a speech). Other possibilities are the excited utterances or even the then-existing conditions exceptions. *See* Tex. R. Evid. 803(2), (3).

Conclusion

Social media is here to stay. Smart business trial attorneys can better serve their clients and add another weapon to their arsenal by applying familiar evidentiary rules to use social media strategically to win trials.

About the Author:

Nick Sarokhanian is a business trial attorney representing businesses and their owners in their significant business disputes. He is a proud husband, father, and Baylor Law graduate. Nick offices in Greenberg Traurig, LLP's Dallas office and can be reached at sarokhaniann@gtlaw.com or at (214) 665-3673.

2015 FTC Guidelines for Data Security

By Pierre Grosdidier and Cassidy Daniels

Cyber-security breaches and data leaks continue to be matters of serious concern to companies and consumers alike. Verizon reported 3,141 data disclosures in 2015, up from 2,122 in 2014.[1] In 2015, Americans reported 490,220 incidents of identity theft, defined as the use or attempted use of another's sensitive Personally Identifiable Information ("PII")[2] to commit fraud.[3] .

The FTC relies on the Federal Trade Commission Act, 15 U.S.C. §§ 41 *et seq.*, for cyber-security oversight, including the right to bring administrative enforcement actions against companies with unreasonable data security practices. Circuit and district court rulings affirming the Commission's jurisdiction over cyber-security practices have bolstered this authority.[4] In 2015 the Third Circuit ruled that the FTC Act grants the Commission authority to challenge "unfair" data security practices.[5] The Commission has aggressively exercised this authority and has brought close to sixty enforcement actions to date.[6]

Other agencies are also concerned with the handling of consumer information—the Department of Health and Human Services' ("HHS") Health Insurance Portability and Accountability Act (HIPAA) sets information security standards for the protection of medical records and personal health information.[7] HHS's Office of Civil Rights enforces the HIPAA

---

1 Verizon, 2016 DATA BREACH INVESTIGATIONS REPORT 1 (2016); 2015 DATA BREACH INVESTIGATIONS REPORT 1 (2015).

2 PII consists of, inter alia, a person's name, address, date of birth, Social Security number, driver's license number, credit card and bank account numbers, phone number, and biometric data

3 Verizon, 2016 DATA BREACH INVESTIGATIONS REPORT 1, *supra* note 1; FEDERAL TRADE COMM'N, GUIDE FOR ASSISTING IDENTITY THEFT VICTIMS 4, (2013).

4 Allison Grande, *LabMD Ruling Puts FTC in Driver's Seat on Data Security*, LAW360 (May 13, 2014, 8:41 PM); *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236, 246-48 (3d Cir. 2015).

5 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d at 248, 259.

6 Opinion of the Commission at 10, n.21, *In the Matter of LabMD*, Docket No. 9357 ("To date, using both its deception and unfairness authority, the Commission has brought nearly 60 data security cases."); Fed. Trade Comm'n, *Commission Statement Marking the FTC's 50th Data Security Settlement* 1 (2014); Leslie Fair, FED. TRADE COMM'N, *Start with Security: New Guide Offers Lessons from FTC Cases* (June 30, 2015, 12:00 PM).

7 U.S. DEP'T OF HEALTH & HUMAN SERVS., *The HIPAA Privacy Rule* (last visited Sept. 9, 2016); U.S. DEP'T OF HEALTH & HUMAN SERVS., *The Security Rule* (last visited Sept. 9, 2016).

Privacy and Security Rules.[8] The Securities and Exchange Commission may also soon be involved in defining and enforcing data security requirements. Senators Jack Reed (D-RI) and Susan Collins (R-ME) proposed a bill in the 114th Congress that would direct the SEC to adopt rules requiring a company to disclose whether it has a cyber-security expert on its board and other measures in place to prevent a data breach.[9]

Given the recent Third Circuit ruling and the FTC's position of authority, and in light of other federal regulatory agencies' increasing attention to cyber-security, businesses should be interested in not only how to prevent a data breach, but also how to mitigate risk in the event of an FTC investigation. This article focuses on the FTC's 2015 rulings involving complaints about data security practices that were considered illegal under the FTC Act.

Ambiguities in Data Security Standards and Liability

The lack of clear-cut universal standards for data security practices has the potential to create ambiguities.[10] The FTC issues complaints against companies for "unfair" data security practices, but what constitutes an "unfair" practice in this area is not clearly defined.[11] Rather, the FTC decides this issue on a case-by-case basis, using a three-part test outlined in Section 5(n) of the FTC Act. ("the Act"). [12] An act or practice may be deemed unfair if (1) it "causes or is likely to cause substantial injury to consumers"; (2) the injury "is not reasonably avoidable by consumers themselves"; and (3) the injury is "not outweighed by countervailing benefits to consumers or to competition."[13] In the recent controversial case of *In re LabMD*,, LabMD disputed the type of harm the FTC was required to show in order to establish a violation of the Act.[14] In this case, a 1,718-page file (the "1718 File") containing medical PII located on a LabMD computer was made available to outsiders via unauthorized peer-to-peer software. The file was reportedly copied only once, but remained accessible for 11 months. In the ensuing

---

[8] U.S. DEP'T OF HEALTH & HUMAN SERVS., *HIPAA Enforcement* (last visited Sept. 9, 2016).

[9] Ted Trautmann, *Call to Action: Planning for the Inevitable Cyberattack*, 19 SEC TODAY 1, 1 (2016). Text of Senate Bill S.2410 available here: www.congress.gov/bill/114th-congress/senate-bill/2410/text.

[10] Allison Grande, *FTC Resolute on Data Security Despite Wyndham Fight*, LAW360 (Sept. 9, 2013, 8:37 PM); Elliot Golding, *FTC Data Security Authority Remains Murky Despite Wyndham*, LAW360 (April 8, 2014, 2:44 PM).

[11] 15 U.S.C.A. § 45.

[12] Golding, *supra* note 10; FED. TRADE COMM'N, START WITH SECURITY 1 (2015).

[13] 15 U.S.C. § 45(n).

[14] *See* Pierre Grosdidier, *Best Practices: The FTC Signals its Intent to Police Big Data*, 79 TEX. BAR JOURNAL 3 (2016); Pierre Grosdidier, *Full Federal Trade Commission Reverses ALJ, Holds LabMD Liable for Data Breach, But Declines to Decide Whether Lax Data Security Breaches Section 5* (Sept. 8, 2016).

proceeding against LabMD, the FTC's Complaint Counsel alleged, *inter alia*, that the mere act of maintaining inadequate security measures on a computer that hosts protected data is enough to breach the FTC Act. Under this test, proof of actual harm caused by identity theft would not be required for liability.[15]

In its Initial Decision, the *LabMD* Administrative Law Judge (the "ALJ") declined "to base unfair conduct liability upon proof of unreasonable data security alone."[16] But the full Commission reversed the ALJ.[17] The Commission found that LabMD breached the FTC Act when it released the 1718 File, even if only once, and when it exposed the 1718 File on a peer-to-peer folder for 11 months. Importantly, the Commission declined to address FTC Complaint Counsel's "broader argument" that a company's inadequate security that potentially exposes PII to a breach is, in and of itself, a Section 5 violation.[18] *In re LabMD* shows how fact-specific the FTC's analyses can and will be. It also shows how low the FTC can set the bar to breach the FTC Act, as the release of the 1718 File occurred only once and led to no known consumer complaints.

Like Wyndham before it, LabMD argued, *inter alia*, that the FTC Act did not provide fair notice of the conduct required.[19] Wyndham, a hotel chain, was hacked three times in a row, resulting in the theft of 619,000 consumer payment card account numbers and $10.6 million in fraudulent charges.[20] In *FTC v. Wyndham Worldwide Corp.*, the Third Circuit Court of Appeals found that Wyndham had fair notice of the standards for data security. However, Wyndham focused its lack of fair notice argument on "the FTC's failure to give notice of its interpretation of the statute" and did not "meaningfully argue that the statute itself fails fair notice principles."[21] The court also stated that respondents are entitled to a low level of statutory notice because Section 45(a) does not implicate any constitutional rights.[22] Wyndham had fair

---

[15] Complaint Counsel Corrected Appeal Brief at ii, *In the Matter of LabMD, Inc.*, 2016 FTC LEXIS 19, No. 9357.

[16] Initial Decision at 86, *In the Matter of LabMD, Inc.*, 2015 FTC LEXIS 272, 186.

[17] Opinion of the Commission at 1, *In the Matter of LabMD*, Docket No. 9357.

[18] *Id.* at 16.

[19] LabMD's First Amended Answer and Defenses to Administrative Complaint at 6, *In the Matter of LabMD*, 2015 FTC LEXIS 184, 8-9; *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 799 F.3d 236, 254 (3d Cir. 2015).

[20] District Court Opinion at 4-5, *Fed. Trade Comm'n. v. Wyndham Worldwide Corp.*, 10 F.Supp.3d 602, 609, No. 13-1887(ES) (D. N.J. 2014).

[21] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d at 255-58.

[22] *Id.* at 255.

notice as long as it could "reasonably foresee that a court could construe its conduct as falling within the meaning of the statute."[23] The court also mentioned that Wyndham failed to follow the practices recommended by a 2007 FTC guidebook for businesses, supporting the conclusion that Wyndham had fair notice.[24]

Wyndham was required to implement a series of security measures detailed by the FTC as part of its settlement terms. Some observers saw this as a step in the right direction in laying out "reasonable" data security practices with more specificity.[25] Because the majority of the FTC's enforcement actions in the data security area are resolved through settlement and consent orders, the FTC has referred to these results as a kind of "common law light" that should inform other companies' practices.[26]

2015 FTC Guidelines

Perhaps in response to complaints regarding the ambiguities of data security standards, in June 2015 the FTC published a set of guidelines for businesses dealing in sensitive consumer information.[27] These guidelines draw from recent FTC settlements and recommend certain policies based on other companies' errors or deficient security practices.

These are not hard-and-fast rules—the FTC recognizes that security practices vary; what is appropriate for a multi-million dollar company handling complex transactions may not be appropriate for a mom-and-pop shop. "The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[28] In *LabMD*, the FTC pointed out that "as the Commission has stated in this case, a company that has maintained reasonable security would not be liable under Section 5 merely because a breach occurred."[29]

---

[23] *Id.* at 256.

[24] *Id.* at 257.

[25] Allison Grande, *FTC Tips Data Security Hand in Wyndham Pact*, LAW360 (Dec. 10, 2015, 10:21 PM).

[26] Julie Brill, Commissioner, Federal Trade Comm'n, Privacy, Consumer Protection, and Competition 2-3, Loyola University Chicago School of Law, 12th Annual Antitrust Colloquium (April 27, 2012).

[27] FED. TRADE COMM'N, START WITH SECURITY 1.

[28] *Commission Statement Marking the FTC's 50th Data Security Settlement* 1, *supra* note 4.

[29] FTC Reply Brief at 16, *In the Matter of LabMD, Inc.*, (citing Order Denying Respondent's Motion to Dismiss at 18 (". . . the mere fact that such breaches occurred, standing alone, would not necessarily establish that LabMD engaged in 'unfair . . . acts or practices.")).

The FTC's guidelines offer the following advice:

- **Do not collect unneeded information.** Hold onto needed information only as long as a legitimate business need exists. LabMD allegedly maintained the personal information of 1,000,000 consumers, for some of whom the company never performed any tests.[30] This practice became part of the basis of the FTC's complaint against LabMD.
- **Restrict access to data.** Twitter provoked an FTC investigation and complaint by allowing almost all employees, regardless of their job duties, to view users' nonpublic tweets and other information and to send tweets on behalf of users.[31]
- **Require secure passwords.** "Qwerty" and "121212" are no better than having no password at all. The Commission was also quick to point out that "at least six employees used 'labmd' as their login password" in its *LabMD* opinion.[32]
- **Suspend or disable users after a certain number of unsuccessful login attempts.** Like the monkeys left alone in a room with a typewriter who will eventually type out all of Shakespeare's plays, hackers use a method that types endless combinations of characters until they luck into the right one. Ten successive failed logins should hint that something nefarious is afoot.
- **Store and transmit sensitive information securely.** Train personnel and use accepted encryption methods—no need to reinvent the wheel. ValueClick, Inc.'s use of a proprietary, nonstandard, and untested form of encryption brought on an FTC complaint and subsequent $2.9 million settlement.[33]
- **Segment networks and monitor who is trying to get in and out.** The FTC brought a complaint against DSW, Inc. for failing to limit computers on one in-store network from connecting to computers on other in-store and corporate networks, making it possible for hackers to use one network to connect to other networks.
- **Secure remote network access.** The FTC brought a complaint against Lifelock, Inc. a company marketing identity theft prevention services, for allegedly failing to require antivirus programs on computers used for remote access to its network.[34] Similarly, mortgage lender Premier Capital Lending, Inc. attracted the FTC's attention by activating

---

[30] Complaint at 2, *In the Matter of LabMD, Inc.*; Complaint Counsel Corrected Appeal Brief at 4, 2016 FTC LEXIS 19, 4.

[31] Complaint at 2, *In the Matter of LabMD, Inc.*

[32] Opinion of the Commission at 2, *In the Matter of LabMD*, Docket No. 9357.

[33] Press Release, Federal Trade Commission, ValueClick to Pay $2.9 Million to Settle FTC Charges (March 17, 2008).

[34] Complaint at 10, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MHM (FTC 2010).

a remote login account for a business client without assessing the client's security, allowing hackers to access the client's system and steal remote login credentials and consumer information.

- **Apply security practices when developing new products or services.** Verify that privacy and security features actually work—test that a photograph will "disappear forever" before promising to consumers that it will.[35]
- **Verify that third-party service providers also use appropriate security measures.** The FTC recommends that businesses insert security standards into their contracts and ensure their partners' compliance.
- **Implement software updates regularly and develop a process to receive and address reports of vulnerabilities.** Another of the FTC's allegations against Lifelock was that it failed to install critical network updates, leaving its network vulnerable to unauthorized access.[36]
- **Do not leave sensitive information out in the open or toss it in the dumpster.**[37] When disposing of equipment or paperwork, devices should be wiped clean and documents should be shredded or burned. The FTC has brought complaints against companies for storing paperwork with sensitive information in boxes in a garage; leaving a laptop with sensitive information in a locked car; tossing paperwork in a dumpster; and selling hard drives without first clearing them.

By and large, it appears that FTC investigations are not triggered by one minor misstep, but by a fundamental failure to implement reasonable procedures to protect sensitive information. Records of FTC complaints and settlements can be found on the FTC's website. The guidelines are available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

These guidelines are a high-level checklist that IT experts may find simplistic or overly general. But this list is a good starting point for a dialog between in-house counsel and IT professionals about the state of data security within a company. The guidelines are also written simply enough for a lay person to understand and then go to the IT professional with questions about

---

[35] Complaint at 2-3, *In the Matter of Snapchat, Inc.*, No. C-4501 (FTC 2014).

[36] Complaint at 10, *FTC v. LifeLock, Inc.*

[37] Press Release, Federal Trade Commission, CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations (Feb. 18, 2009).

what kind of data protection exists and what improvements are necessary in the future to meet the FTC's expectations.

About the Authors:

Pierre Grosdidier is an Attorney in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. His practice focuses on complex commercial litigation, especially lawsuits and arbitrations with strong technical elements. He has litigated cases involving the Computer Fraud and Abuse Act and the stored Communications Act, and also trade secret, construction, oil and gas, and software copyright claims. Pierre is also a member of Haynes and Boone's Privacy and Data Breach focus group. Prior to practicing law, Pierre worked in the process control industry straddling refining, automation, and software. 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 and is a registered Texas P.E. (inactive).

Cassidy Daniels is an attorney in Haynes and Boone, LLP's Business Litigation practice group in San Antonio, Texas.


COMPUTER AND
TECHNOLOGY
SECTION

* Tech Tips *

Keyboard Shortcuts for Word

- Ctrl C — copy selected text
- Ctrl X — cut selected text
- Ctrl V — paste previously copy or cut text
- Ctrl Z — undo previously performed actions; can be repeated multiple times
- Ctrl Y — redo what was previously undone via Ctrl Z
- Ctrl B — bold selected text
- Ctrl I — italicized selected text
- Ctrl F — search for text
- Ctrl H — find and replace text
- Ctrl G — go to a page, section, line, etc.
- Ctrl E — center text
- Ctrl L — left align text
- Ctrl R — right align text
- Ctrl J — justify text
- Ctrl N — open a blank document while keeping the current document open
- Ctrl S — save document
- Ctrl Home — go to the beginning of a document
- Ctrl End — go to the end of a document
- Ctrl 1 — change to single line spacing
- Ctrl 2 — change to double line spacing
- Ctrl 5 — change to 1.5 line spacing
- Ctrl] — increase font size of text
- Ctrl [— decrease font size of text
- Ctrl = — subscript text
- Ctrl shift = — superscript text
- Shift F3 — change the case of text

Set up a custom keyboard shortcut for Word in a PC

Using the Strikethrough function as an example:

1. Press Ctrl D to bring up the Font dialog box
2. Press Ctrl Alt and press + (plus sign) key on Numeric Pad
   * cursor will change to a clove shape
3. Click on the Strikethrough option in the Font dialog box
   * customize Keyboard dialog box will open
4. Place cursor in the "Press new shortcut key" box, and press any combination of Shift, Alt, Ctrl key(s) and a letter key (e.g., Ctrl Shift S) as a desired shortcut key combination for the Strikethrough function
5. Click on Assign button in the Font dialog box to set Ctrl Shift S as the shortcut for the Strikethrough function

Mouse shortcuts for Word

- Select a word — double click on the desired word
- Select a sentence — hold down Ctrl key and click once within the sentence
- Select a paragraph — triple click on the desired paragraph

Insert special characters via keyboard

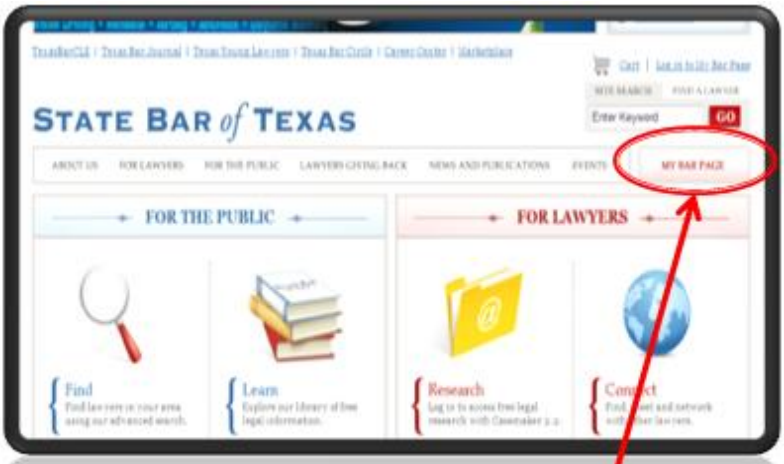
- em dash — — Alt Ctrl – (minus sign)
- en dash ¬– — Ctrl – (minus sign)
- section symbol § — Alt Ctrl 21
- copyright symbol © — Alt Ctrl C
- trademark symbol ® — Alt Ctrl R
- ellipsis … — Alt Ctrl . (period)
- single opening quote ‘ — Ctrl ` (single quotation mark), then ` (single quotation mark)
- single closing quote ’ — Ctrl ' (single quotation mark), then ' (single quotation mark)
- double opening quote “ — Ctrl ` (single quotation mark), then " (double quotation mark)
- double closing quote ” — Ctrl ' (single quotation mark), then " (double quotation mark)

Insert symbols and special characters via Symbol Box

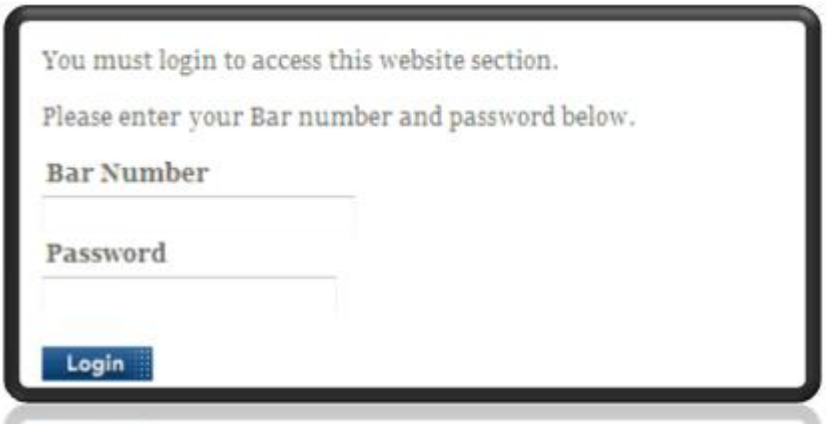
1. Go to Insert > Symbol to open Symbol box
2. Locate the desired symbol and double click it to insert the desired symbol at the current cursor position

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

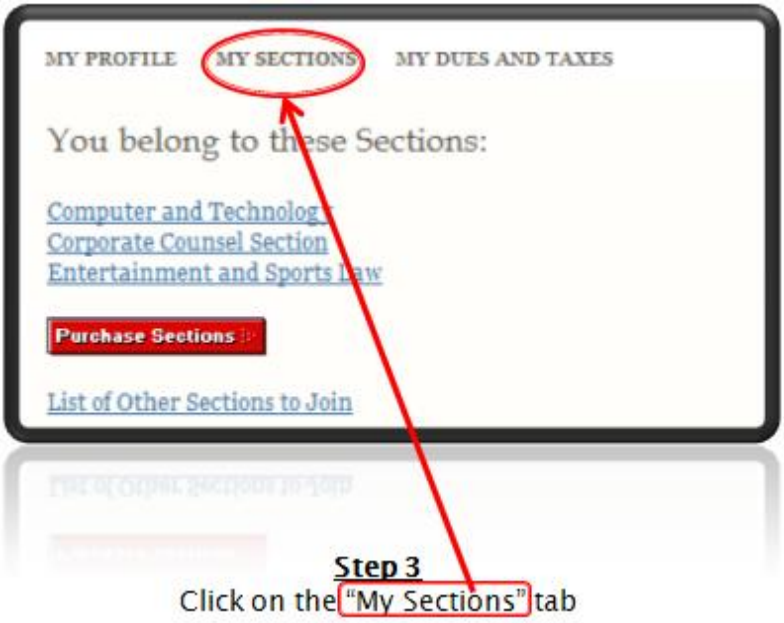
Joining the State Bar of Texas Computer & Technology Section is easy. You can join online by visiting the State Bar of Texas Website at www.Texasbar.com. Please follow these instructions to join the Computer & Technology Section online.



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

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

Term Expiring 2017

Elizabeth Rogers– Austin
Shawn Tuma – Dallas
Bert Jennings – Houston

Term Expiring 2018

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

Term Expiring 2019

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

Chairs of the Computer & Technology Section

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