COMPUTER AND TECHNOLOGY SECTION

Circuits

e-Journal of the Computer & Technology Section
of the State Bar of Texas
June 2021

Table of Contents

Featured Articles

Short Circuits

Circuitboards

Table of Contents

Feature Articles:-

Short Circuits:-

Circuitboards:-

Message from the Chair

By Shawn E. Tuma

Welcome to another issue of *Circuits*. As I conclude my term as Chair of the Computer & Technology Section, I first want to thank all of the Section Members for the wonderful opportunity to serve as Chair of the Section for the 2020-2021 Bar year; it has been a tremendous honor for me.

As I reflect on the events of this past year, I initially think of the Covid-19 Pandemic and how much our world has changed over this past year and how integral technology has been in that process. I think of the impact the Pandemic had on the way all of us live and work, and the outstanding work of our Section in rising to the occasion by educating members of the Bar on different tools and techniques to not only adapt, but to thrive in this new environment. Now, as we are seeing the Covid-19 Pandemic begin to wind down (hopefully) and restrictions being lifted, we are seeing another pandemic come to the forefront.

In May of 2021, a watershed event occurred that brought cybersecurity and the global ransomware pandemic front and center in the minds of ordinary Americans. The ransomware attack on the Colonial Pipeline shutdown roughly half of the fuel supplies for the U.S. East Coast and triggered concerns of a national fuel shortage. With this pandemic, however, instead of panic-buying toilet paper, people were panic-buying gasoline and attempting to store it in things like plastic containers, buckets, and even trash bags! This behavior was so rampant that the US Consumer Product Safety Commission had to issue a warning against such practices.

While those of us who routinely work in cybersecurity have been warning against ransomware for several years, the attack on Colonial Pipeline was different. This event brought the ransomware pandemic home to the masses much like the data breaches of Target, Home Depot, and Neiman Marcus did for the data breach issue back in 2013. Now, people are beginning to understand that even if they (falsely) believe that it will not happen to them (it can!), even when such attacks happen to others, they can and will be affected in ways that they cannot even envision. Cybersecurity — and ransomware in particular — is truly a national security issue that impacts each and every one of us, our law practices, our clients, and our nation — all of which are critical to preserving our way of life.

The intersection of law and technology is as critical now as it has ever been, and the Section has been on top of the ransomware issue and producing valuable content for our Members. The very first presentation of our 4th annual *With Technology and Justice for All* conference last

December was titled "Ransomware – a True Existential Threat to Your Practice!" with Lavonne Hopkins, of Dell Technologies, FBI Supervisory Special Agent Brett Leatherman, and myself as presenters. Volume 17 of Circuits, published last November, featured the article *With Ransomware Attacks Increasing, Cyber Insurance Now Seen as a Necessity, Not a Luxury*, and we have TechBytes on ransomware and basic cybersecurity tips to help those at every level of tech sophistication better protect themselves against this risk.

Our State Bar Annual Meeting occurred virtually in June and provided outstanding programming featuring many Section Members on a broad range of cutting-edge law and technology subjects, including the popular Adaptable Lawyer Track. I hope that you had an opportunity to join in and catch some of this programming.

We invite you to join us and actively participate in the work of the Section through one of our Committees and Working groups. This will allow you to get more involved and contribute to the work of the Section. We are actively seeking new members for the following:

- Membership, Orientation & Outreach Committee
- Diversity Committee
- Social Media, Communications and Marketing Committee
- CLE Working Group
- Circuits Working Group
- Tech-Bytes Working Group
- The App & Strategic Partnerships
- In-House & Government Counsel Working Group
- Solos & Small Firms Working Group
- Cyber | Privacy | eCommerce ADR Working Group
- Cybersecurity & Privacy Working Group
- eDiscovery Working Group
- Emerging Technology Working Group
- Tech Competence in Practice Working Group
- Tech in the Courts Working Group

I now have the privilege of passing the Section's "virtual" gavel to my dear friend and our incoming Chair, Elizabeth Rogers. While I have no doubt that Elizabeth will continue to be the great leader she has already proven herself to be and will be remembered for many great accomplishments during her term as Chair, I want to also congratulate Elizabeth on being the first female Chair in the history of our Section! Congratulations, Elizabeth!

I also want to recognize both Lisa Angelo and Ron Chichester with the Chair's Recognition Awards for 2021: Lisa in recognition of her commitment and contributions to the Computer & Technology Section and growing the membership and developing strategic partnerships, and Ron in recognition of his commitment and contributions to working on the technology of the Computer & Technology Section by keeping it "ticking" through the years. Congratulations, Lisa and Ron!

Thank you again for your membership and for your interest in matters at the intersection of technology and the law. If you would like to become more involved in the Computer & Technology Section or have other ideas you would like to share, please contact our Section administrator at admin@sbot.org.

It has been an absolute honor and a pleasure to serve as your Chair for this past year. Thank you very much.

Shawn E. Tuma
2020-2021 Chair
Computer & Technology Section
State Bar of Texas

Letter from the Editor

By Sanjeev Kumar

Welcome to the final issue of *Circuits* for the 2020–21 Bar year!

In our Feature Articles, we start with a contribution from our outgoing Chair, Shawn Tuma, discussing the nature of cybersecurity threats. The article provides a historical perspective on cybersecurity threats and is a timely reminder to our audience considering the recent attack on Colonial Pipeline resulting in shortages and panic-buying of gas throughout the southeast region of the country.

The next article is penned by a guest author, Griffin Weaver, in which he discusses the important aspects of how best to protect attorney-client privilege for information discovered and created in internal investigation as a consequence of a cyberattack and in preparation for possible ensuing litigation. The article provides helpful guidelines in managing such an investigation for attorneys providing advice to corporate clients who may fall victim to a cyberattack.

We have experienced a significant explosion of Mobile Apps. Whatever the consumer wants, there seems to be an app for that. This has resulted in some novel legal issues associated with product liabilities. In the next feature article, our immediate past chair, John Browning, discusses the trends in products liability associated with downloaded apps, as well as the added complexity due to subtle differences in products liability laws in different states.

For cryptography buffs, our past chair, Craig Ball, discusses the topic of steganography in the next feature article. The article provides a basic understanding presented in an easy-to-understand narrative as how a piece of text or image carry a lot more information than what is visible at first glance and can be used to convey information in secret.

We start our *Short Circuits* section with a short article by our past editor and council member, Pierre Grosdidier, which discusses the Fourth Amendment rights related to drone surveillance in light of some recent court decisions.

There has been a huge proliferation of digital devices and wearable tech which are almost becoming ubiquitous in our daily lives. John Browning brings to us multiple articles in *Short Circuits*. In his first offering, John discusses the evidentiary issues created as a consequence of use of such devices and the use of data in litigation that is being created and stored through the use of such technology. In his next contribution, John provides a glimpse into the misuse

of available technology by misguided individuals with special focus on obsessive parents trying to provide an unfair advantage to their children.

Considering the frequent disasters in Texas in the last few years, the last one being the "Icepocalypse" earlier this year, the next article in *Short Circuits* by John Browning provides some helpful guidelines for attorneys to be prepared for such disasters and disaster-proof their practice.

Our next *Short Circuits* article is also penned by Pierre Grosdidier. He provides a summary of the recent U.S. Supreme Court decision in "*Van Buren v. United States*," in which the Court interpreted the language of the Computer Fraud and Abuse Act pertaining to what constitutes exceeding authorized access.

The next two *Short Circuits* articles are contributions from John Browning discussing the constitutionality of the Texas Revenge Porn Law and the culpability of online retailers under products liability claims respectively.

Ever wonder what the bar codes and QR codes on the products that we purchase on a daily basis mean? Our sole *Circuitboards* article is penned by our past chair, Craig Ball, in which he sheds light on the technology underlying the bar codes and QR codes.

Many thanks to all the contributors to this new issue. Thanks to Kirsten Kumar for her review of and assistance with this issue's articles. We hope that you enjoy this new edition of *Circuits* and as always, we welcome any comments that you may have. The accomplished members of the Computer & Technology Section Council are always willing to help in any way possible. Please do not hesitate to contact us, be it a comment or a request for assistance, through our section administrator at admin@sbot.org.

Kind Regards,
Sanjeev Kumar, Co-Editor

The Nature of Cybersecurity and Strategies for Unprecedented Cyber Attacks

By Shawn Tuma

What is foreseeable is that cyber-attacks often are not. The conditions for the attacks almost always are, but the actual attack itself is not; otherwise, appropriate steps would have been taken to prevent the attack. Put another way, any CEO who knew her company would be hit with a successful ransomware attack tomorrow night would move Heaven and Earth tomorrow to protect against the attack.

Several years back, the Sony Pictures Entertainment (SPE) hack turned on its head the business world that was already trying to come to grips with the Home Depot, Target, Neiman Marcus, and many other data breaches. There was one thing about the SPE breach that really had the cybersecurity community in quite a buzz.

An internal email from SPE's cybersecurity investigators was made public and some were taking it as saying "It's okay, it could have happened to anybody and there was nothing Sony could have done to stop it. It is not Sony's fault." That inference came from statements in the email that referred to the attack as being *unique* and *unprecedented* with the malware being undetectable by *industry standard antivirus software*.

While such statements have become the norm today, the kerfuffle that ensued from SPE brings to mind the bigger picture of cybersecurity. Things such as what I have been preaching about cybersecurity. What others have been preaching about cybersecurity. More directly, what our respective roles are when it comes to cybersecurity and where and how (or whether) we really provide value to our customers and clients.

Without opining on the particular exculpatory statements relative to SPE or any other particular breach event, I invite you to join me in considering how words such as "*unique*" and "*unprecedented*", and concepts such as *industry standard antivirus software* fit into the bigger picture of cybersecurity. For me, it began with a question:

> But for the unique and unprecedented nature of most substantial cyber-attacks, would there be a need for our professional experience, knowledge, and judgment in developing cybersecurity strategy?

As we sit here today, should we not anticipate that attacks against companies will be unprecedented, damaging, unique attacks that both steal data and do harm to the victim of the attack? Consider these excerpts from a law review article that I published in 2011[1] in which I argued that this is what we should anticipate:

> * * *
>
> Business and warfare are one and the same. That, we were told in the '80s by Gordon Gekko, and, after all, the object is the same: to win–to defeat your enemy. Borrowing from the lessons of a true warrior, he further elucidated that the key to winning was to plan ahead and think about the strategy before entering the battle, because "[e]very battle is won before it is ever fought."
>
> Gekko attributed this to the lessons of Sun Tzu, who indeed taught that preparation is the key to winning:
>
> > *Now the general who wins a battle makes many calculations in his temple before the battle is fought. The general who loses a battle makes but a few calculations beforehand. Thus do many calculations lead to victory, and few calculations to defeat: How much more do no calculation at all pave the way to defeat! It is by attention to this point that I can foresee who is likely to win or lose.*
>
> Regardless of the source, the principle remains the same and is, almost without fail, a truism that applies equally to war, business, and litigation. Preparation is the key to winning.
>
> In today's business environment, businesses are in a perpetual state of warfare. Competition is the essence of business. Honest competition is beneficial, as it drives efficiency and innovation. Unfortunately, dishonest competition is not.
>
> Corporate espionage, corporate sabotage, and corporate theft have become part of the business landscape as well; those that cannot prevail through honorable means of competition often resort to dishonorable means to take customers, employees, and information.

---

[1] Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?" A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S. CAROLINA L.R. 141 (2011), https://scholarcommons.sc.edu/sclr/vol63/iss1/6/.

This has become a way of life in business and is frequently being accomplished through the use of computers to commit dishonest acts of deception, i.e., computer fraud.

The risks are certainly not limited to only those from corporate competitors. They also come from others engaged in computer fraud–thieves, hackers, anarchists, and inquisitive amateurs–who all pose a significant risk, and whose weapon of choice is also the computer.

Computer fraud is a rapidly growing threat to businesses.[2]

* * *

Many nations are already convinced [that computer technology is the wave of the future] and have prepared their armies for war on the cyber battlefield. The world's militaries have used computers for decades, and they are an integral component of virtually all modern military systems.

Despite this fact, society has now taken another quantum leap forward. The close of the first decade of the New Millennium saw a formal change in the art of warfare that, for the first time in history, moved the battlefield from the physical to the cyber arena.

One needs little imagination to suspect that the world's militaries have been engaged in cyber warfare for as long as computers have been in use; however, it had not become official. The year 2010 saw the first weaponized computer virus used to hamper Iran's nuclear ambitions. Though people knowledgeable of cyber warfare have expected such a cyber-attack for years, it has finally happened: Stuxnet.

The Stuxnet virus has been called "the most sophisticated cyberweapon ever deployed." Stuxnet was a computer worm designed to use a variety of "previously seen individual cyber-attack techniques, tactics, and procedures, automate them, and hide its presence so that the operator and the system have no reason to suspect that any malicious activity is occurring." Stuxnet was so sophisticated that it was designed to eliminate all traces of its existence. This is a serious weapon.

We are well over half a century into the Computer Age and we have seen the first change from the physical battlefield to the cyber battlefield. This is the first time since the dawn

---

[2] *Id.* at 142–43.

of mankind that battles have been fought somewhere other than on an actual battlefield–now in cyberspace.

While no nation has claimed responsibility for the Stuxnet attack on Iran, and no one knows for sure, many experts believe it was a joint operation led by the United States and Israel, with help from Germany, and perhaps others.

As Stuxnet has shown, over the past year, warfare has changed. There is a new weapon that has, at least on one occasion, replaced missiles, bombs, and ground troops: computers. Now, in the wake of Stuxnet, some security experts have begun to express fear that the attack has "legitimized a new form of industrial warfare, one to which the United States is also highly vulnerable."

Just as the United States is vulnerable, so too are businesses within the United States and around the world. Just as the computer is increasingly becoming the weapon of choice for warfare, so too has it in business warfare.

Computers are being used for corporate espionage (manipulating and stealing data), corporate sabotage (stealth attacks through computer viruses), or any number of other methods of attacking enemies' (competitors) strengths or exploiting their weaknesses, including old fashioned theft. . . . While many of the illicit tactics that businesses use to attack each other are often classified as crimes and punishable by criminal law, in the civil realm they are generally classified as fraud. What is even more troubling is that these attacks come from inside, as well as outside, of the businesses that are attacked.[3]

* * *

Substantial Cyber Attacks Often are Unique and Unprecedented – That is Why They Are Successful

Wasn't the Stuxnet attack on Iran unprecedented in nature? Wasn't the Target hacker's strategy of using Target's less well-defended HVAC vendor–Fazio Mechanical–to gain an entry point into Target's network[4] an unprecedented attack based upon what we knew at that time? Wasn't the Heartland breach in 2008 an attack that was sophisticated and unprecedented in nature

---

[3] *Id.* at 145–47.

[4] Shawn E. Tuma, *Corporate Espionage: Hacking a Company Through a Chinese Restaurant Takeout Menu* (Apr. 15, 2014), https://shawnetuma.com/2014/04/15/corporate-espionage-hacking-a-company-through-a-chinese-restaurant-takeout-menu/.

based upon what we knew at that time? Now, in the wake of the FireEye / SolarWinds attack,[5] would anyone argue that it was not sophisticated and unprecedented in nature?

All were. At the time they were unknown-unknowns. They involved strategies and techniques that the victims did not yet know even existed. They did not know what they did not know. What we learned from this is that what is foreseeable is that cyber-attacks often are not foreseeable. Thus, look for the unexpected.

Industry Standard Antivirus Software is Not – and Was Not – Effective Against Unknown Unknowns

Even at the time of the SPE cyber-attack it was well understood in the security industry that antivirus software, by design, would only defend against known-knowns; that is, the low hanging fruit kind of malware that was already known, with its signature identified and updated in the AV software databases.

Most significant cyber-attacks are (and were) designed to be unique and unprecedented to enable them to circumvent and evade antivirus software. That is what makes them so challenging. That is exactly why cybercriminals use them in that way.

But, isn't that also why the cost of antivirus software is in the hundreds of dollars while the cost for real-life security professionals is much more? Isn't that the point that so many of us have been trying to make: simply installing and maintaining AV software is not enough. Indeed, is there any single tool that is enough? Many vendors will try and sell the proverbial silver bullet but, in reality, there is no such silver bullet and, even if there were as of the time of this writing, it would not be by the time you are reading this – that is the nature of cybersecurity.

The Nature of Cybersecurity

Combatting the unique and unprecedented nature of business cyber risks is the essence of cybersecurity. Cyber risks are continuous and evolving; therefore, cybersecurity and cyber risk management must also be a continuous process that is always evolving to anticipate and defend against the threats. This work is never done. Such is the nature of cybersecurity.

---

[5] Shawn E. Tuma, *A Lesson in Humility from the FireEye and SolarWinds Cyber Attack,* Ethical Boardroom, https://ethicalboardroom.com/a-lesson-in-humility-from-the-fireeye-and-solarwinds-cyber-attack/.

When defending against cyber risks, there are known-knowns that we can prepare for and there are unknown-knowns that we can learn about and then prepare for to a certain degree. But, there are also unknown-unknowns that do not even exist at this moment but that are quickly becoming unknown-knowns. These are the real challenge.

Cybersecurity is a Lot Like Law – It Requires Experience, Knowledge, and Judgment to Be Effective

In his Introduction to *The Nature of the Judicial Process*,[6] the great jurist Benjamin Cardozo explained the value of applying experience, knowledge, and judgment to solving problems in the law. This reasoning is equally applicable to cybersecurity:

> *[T]he work of deciding cases in accordance with precedents that plainly fit them is a process similar in its nature to that of deciding cases in accordance with a statute. It is a process of search, comparison, and little more. Some judges seldom get beyond that process in any case.*
>
> *Their notion of their duty is to match the colors of the case at hand against the colors of many sample cases spread out upon their desk. The sample nearest in shade supplies the applicable rule. But, of course, no system of living law can be evolved by such a process, and no judge of a high court, worthy of his office, views the function of his place so narrowly.*
>
> *If that were all there was to our calling, there would be little of intellectual interest about it. The man who had the best card index of the cases would also be the wisest judge. It is when the colors do not match, when the references in the index fail, when there is no decisive precedent, that the serious business of the judge begins.*

Similarly, the ability to use experience, knowledge, and judgment to help clients prepare for and defend against unknown-unknowns is where our real value lies. It is where the serious business of the cybersecurity professional begins.

Indeed, this is the very reason why we invest so much time and effort into educating the Boards of Directors and the C-Suites of companies to help them understand that simply relying on AV software or any other tool *de jure* is not enough. This is why we tell them they need to

---

[6] Benjamin N. Cardozo, *The Nature of the Judicial Process* (Lecture I. Introduction. The Method of Philosophy) (1921), Yale University Press, https://constitution.org/1-Constitution/cmt/cardozo/jud_proc.htm

take business cyber risk seriously and make a substantial investment in cybersecurity, their cyber risk team, and their overall cyber risk management program, which must be continuously maturing.

If we are unable to help companies develop a cybersecurity strategy for unique and unprecedented cyber-attacks, how does our experience, knowledge, and judgment provide any value to our clients? When asked about what helped him be so effective, the great Wayne Gretzky said, "I skate to where the puck is going to be, not to where it has been."

Isn't that what we are telling companies' Boards and C-Suites that we can help them do? Not that we are here to report on and defend against what is already known—where the puck has been—but to use our experience and judgment to help them better predict what we believe *could* be unknown-unknowns—where the puck may be going? Isn't that where our real value lies?

Cybersecurity is not a science, it is an art. It is not based on a formula. Often, there is no right answer and there is no wrong answer. It is a question of knowledge, experience, and judgment. And, there are times when we will fail. That is part of being a professional practicing an art.

But there are also times when we will prevail when many would not have. These questions of judgment are what distinguishes a professional from a technician and, while it is extremely challenging and many times thankless, that is the nature of the security process.

About the Author

Shawn Tuma is a partner at Spencer Fane LLP in the firm's Dallas and Plano offices. He helps businesses protect their information and protect themselves from their information, representing a wide range of clients, from small to midsize companies to Fortune 100 companies, across the United States and globally in dealing with cybersecurity, data privacy, data breach and incident response, regulatory compliance, computer fraud-related legal issues, and cyber-related litigation.

Data Breach Forensic Reports: How Do We Protect Them Now?

By Griffin Weaver

In 2015, a federal district court in Minnesota appeared to clarify how companies should conduct breach response to preserve privilege. That court, in what is more commonly known as the *Target* case, denied a plaintiff's motion to disclose documents generated during Target's investigation of its massive 2013 breach. The court explained because Target created a two-track investigation – one for the non-privileged investigation, tasked with understanding and responding to the breach, and the other for the privileged investigation, tasked with preparing the company for anticipated litigation and regulatory inquiry – the documents generated for the second track were protected by attorney-client and work product privileges.[1]

As a result of this ruling, many in-house counsel and law firms wrote and advised their clients to set up these two-track investigatory processes – believing that this would ensure certain data breach reports would remain protected from disclosure. This belief, for the most part, lasted until this past May, when a federal court in Virginia, following a couple of recent rulings by other courts, shocked the legal and security communities when it ordered Capital One to release its attorney-supervised post-breach forensic report that a cybersecurity firm made following the company's massive 2019 data breach.[2] Capital One's position was that they, like Target, had followed a two-track investigation – one track being led by Capital One's cyber incident response team, tasked with understanding and responding to the breach, and the other led by their outside counsel Debevoise & Plimpton, tasked with preparing the company for anticipated litigation.[3] They also explained that work-product privilege doctrine shielded the post-breach report because Debevoise had initiated, directed, and received the analysis as part of that firm's own investigation into the breach. Specifically, Capital One showed that (1) Debevoise engaged an outside forensics firm, Mandiant, to help the firm prepare for litigation, (2) Debevoise specified in its engagement letter with Mandiant that it would direct and receive Mandiant's work in order to render legal advice, (3) Capital One walled off the Mandiant team

---

1 *In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522, 2015 WL 6777384, at *1 (D. Minn. Oct. 23, 2015).

2 *In re: Capital One Customer Data Sec. Breach Litig.*, MDL No. 1:19md2915 (E.D. Va. May 26, 2020) (mem. op.).

3 *Id.*

from Capital One's cyber incident response team, and (4) Capital One paid for the work from its legal department's budget.[4]

The court, after ordering disclosure of the report, noted that privilege will protect documents, like the forensics firm's breach report, only when the documents distinctively reflect preparation for litigation. The burden was on Capital One to distinguish the report's content from what would appear in a report issued for a normal business purpose, if a lawsuit was not an issue. When performing this comparison, the court did not find a distinction between the two. Instead, it found evidence showing similarities, namely:

- Capital One's existing relationship with Mandiant, which pays the forensics firm an annual retainer for incident work that is labeled a "business-critical" expense instead of a "legal" one.
- Capital One's agreement with Mandiant, which was entered into before the incident, and the Debevoise-drafted agreement, executed after the incident, looked functionally the same.
- Capital One originally paid Mandiant's fees with its existing retainer, only later adjusting its budget designation to Legal.
- Capital One provided the forensic report to its outside auditor, four different banking regulators, and select members of Capital One leadership.

In January, the federal district court in the District of Columbia followed suit, ruling that a forensic report was not protected by the attorney-client and work product privileges.[5] In that case, a law firm, Clark Hill, PLC, suffered a cyberattack in which hackers sponsored by the Chinese government broke into Clark Hill's computer network and stole personal information concerning the plaintiff, Guo Wengui, including an application for asylum the Chinese billionaire had submitted to the U.S. government.[6] The court ordered Clark Hill to hand over the forensic report that its forensic firm, Duff & Phelps, had expressly prepared for its outside counsel.[7]

---

4 *Id.*

5 *Wengui v. Clark Hill, PLC*, No. 19-3195, 2021 U.S. Dist. LEXIS 5395 (D.D.C. Jan. 12, 2021) (mem. op.).

6 *Id.*

7 *Id.*

Similar to the defendants in the *Target* and *Capital One* cases, Clark Hill claimed that it had used a two-track investigation, non-privileged and privileged, when investigating the breach.[8] In reaching its decision, the court relied on several key pieces of evidence:[9]

- Clark Hill's forensic firm, eSentire, failed to complete an investigative report to round out the non-privileged efforts;
- eSentire did not conduct a full investigation into the incident;
- Clark Hill stated in an interrogatory response that "its understanding of the progression of the September 12, 2017 cyber-incident is based solely on the advice of outside counsel and consultants retained by outside counsel" (emphasis in original); and
- Clark Hill distributed this second, purportedly privileged report, for a "range of non-litigation purposes."

The court concluded that the forensic report would have been created in the same fashion for business reasons, were no litigation possible.[10]

How to Protect Forensic Reports Going Forward

The *Capital One*, *Clark Hill*, and other recent decisions present a problem for attorneys seeking to maintain the ability for clients to freely communicate while also allowing a company to contract a forensics vendor in a time-sensitive environment. As attorneys consider methods for contracting incident response forensic support, the *Capital One* and *Clark Hill* cases are instructive.[11] The following, derived from the *Capital One*, *Clark Hill*, and other recent court decisions, constitute certain steps attorneys may want to consider in preserving privilege amidst the realities of heightened judicial scrutiny.

Preparation

A. Plan for a Two-Track Investigation

One method of protecting the privilege is a two-track investigation – one tasked with understanding and responding to the breach and the other tasked with preparing the company for anticipated litigation and regulatory inquiry. The incident response plan should outline that counsel is responsible for hiring, directing the activities of, and paying (from its budget) the

---

8 *Id.*

9 *Id.*

10 *Id.*

11 It is important to note that, at the time of this article, the *Capital One* and *Clark Hill* courts appear to be in the minority; however, they may be predictive of what is to come.

forensic team tasked with preparing the company for anticipated litigation and regulatory inquiry. The other team should be paid from a business budget (e.g. security department's budget). The company may also want to consider having this team on retainer for speed and efficiency purposes.

Decide whether the plan will utilize one or two different forensic firms in the two-track investigation. Several courts have viewed the hiring of a second firm as a significant factor when deciding whether to protect a forensic report as litigation work product. However, the recent *Capital One* and *Clark Hill* decisions appear to downplay this significance, skeptically labeling this approach as a "papered" tactic.

Utilizing only one forensic firm for investigation has the advantage of institution familiarity, which enables the firm to operate with much higher speed and efficiency in investigating the incident. However, this approach typically involves the handover of supervision of the firm to counsel immediately after the breach, which several courts, over the years, have viewed as artificial – undercutting the claim of privilege. If cost or other reasons prevent a two-firm approach, make sure your plan still calls for a two-track investigation with two separate teams – with different names, personnel, and, if possible, locations. Prepare two specific engagement letters and statements of work – one for the team covering the response to the breach and the other for the team responsible for preparing the company for anticipated litigation and regulatory inquiry.

B. Get in Front of Potential Forensic Firm Payment Issues

As mentioned above, recent court decisions have not viewed the one-firm approach favorably. Practically speaking, the one-firm approach is the most common and cost-effective. Yet, courts often fail to understand the business reasons for working with a single vendor, as well as the impracticalities around the two-firm approach. In the forensic world, many firms will not engage or respond quickly unless the company has a retainer with the firm. These retainers can reach into the hundreds of thousands of dollars and are often "use or lose it" – meaning if the value of the retainer is not spent within a specific period (e.g. 12 months), the company loses it. Unless a major data incident occurs, legal departments would have no use for forensic firm services. For that reason, companies have incentive to contract using the security department budget.

Counsel may want to consider a few of the following approaches to address the impracticalities of the two- firm approach. One option is to use the one-firm approach outlined above and work with the firm and your accounts payable department to make sure payment for the

privileged track comes from the legal department without error. A second option is to retain an outside counsel firm that has a forensic firm on retainer. This will allow the legal department to use the retainer on other legal services in the event the legal department does not have any need for a forensic firm.

C. Train and Practice with your Teams

Counsel should strongly consider running regular table-top exercises with applicable and external teams. This allows counsel to correct poor communication and process practices that will put privilege at risk. A live incident is not the time to work out the "kinks." Consider scheduling at least one table-top exercise that focuses on following a two-track investigation, training the teams on how to communicate, and appropriate processes to follow.

Track One: Understanding and Responding to the Breach (Non-Privileged) Track

Immediately upon learning of the incident, counsel will want to work with the company's incident response team to create a statement of work for the forensic team tasked with understanding and responding to the breach. This statement of work should emphasize mitigation and remediation tasks that allow the company to continue and resume operations during the incident.

A. Oral Reports

As mentioned above, the team should be trained to perform initial reports orally. These initial reports should address subjects such as: immediate mitigation activities (i.e. how to stop the attack, secure systems, and limit additional damage) and immediate remediation activities (i.e. system restoration, patching, and clean up).

B. Only the Facts

As noted by the court in *Clark Hill*, the company has a business need to determine the source and extent of the attack. The team, when communicating this information in reports, should focus on the facts. Counsel may want to consider reminding the team that their written reports should exclude any subjective judgments or interpretation of the facts. The facts covered in the report can include:

- the indicators of compromise;
- the attacker's progression through the network and systems;
- impacted software or applications; and
- evidence left by the attackers, *e.g.*, logs, trademarks, etc.

Topics which should be excluded focus on subjective information. Examples are:

- the descriptions of the attack vectors;
- the techniques and tactics used;
- the extent of the information exfiltrated;
- attacker attribution;
- overall effect of the attack on the IT infrastructure and cybersecurity program; and
- theoretical or unclear determinations of the damage to hardware or software.

C. Carefully Craft the Written Report

Counsel should strongly consider working with the team to help guide what technical details and company facts are included in the non-privileged report. Any discussion around or comparison of the company's information security practices to industry standards, recognized frameworks, or regulatory requirements should generally be avoided. To avoid a court viewing the report as a "whitewash," counsel may want to make sure the report includes generous amounts of technical detail such as logs, attack progressions, and the technical response steps the company took. It should also include some of the team's interpretations and conclusions about the facts that carry a high level of confidence. This report, or a derivative of it, is designed to brief the business and executive management, and should be tailored as such.

Track Two: Preparing for Anticipated Litigation and Regulatory Inquiry (Privileged) Track

This track should work concurrently with track one. Upon learning of the incident, counsel should strongly consider drafting an engagement letter and scope of work for the forensic team tasked with helping to prepare the company for anticipated litigation and regulatory inquiry.

A. Engagement Letter and Scope of Work

The engagement letter and scope of work should specifically call out the following:

- The team will be a part of the legal investigation team;
- Payment will come from counsel via its legal budget;
- The work is being directed by counsel and performed to prepare for litigation;
- Any dissemination of the work performed or information gathered will be at the discretion of counsel; and
- The scope of the work is separate from any remediation or regulatory work and is explicitly limited to that which helps the legal defense in interpreting the legal consequences of the incident.

In the event only one firm is being used, the engagement letter and scope of work should also call out that (1) any remediation services will be handled in a separate letter of engagement and work statement with the forensic firm, and (2) that the assigned team should not reach out to or discuss the engagement with anyone else outside team, particularly those from the firm performing the other track of work.

B. Specify Communication Protocols

Like track one, initial reports should be performed orally. Any subjective judgments or interpretation of the facts by the forensic team about the company's preparation, response, and practices should be made orally and excluded from email or written messages.

After the forensic team has had adequate time to investigate, counsel may ask the team to convey its findings in writing – in the form of privileged letters to counsel, not reports. In the event the company is only producing one report or prefers an additional measure of protection, the counsel may direct the team to draft a summary report of the technical information and facts incident. Counsel may then use that report as an appendix to the larger privileged report.

C. Drafting the Privileged Report

The privileged report should consist of counsel's analysis of the forensic evidence about the company's behavior before and during the breach. Counsel will want to blend the facts with their analysis throughout the report. Additionally, throughout the report, counsel will want to weave the forensic findings in an analysis referencing contractual obligations, legal standards and case law, and reasonableness.

Depending on the method of attack, analysis should include:

- The jurisdiction of the customers impacted;
- Notification obligations associated with the incident;
- Whether any of the company behavior constitutes negligence;
- The reasonableness of the cybersecurity efforts under legal standards and industry practices; and
- Appropriateness of the forensic team's recommendations for improving the company's technical and security postures.

D. Tightly Control Distribution of the Reports

As exhibited in the *Capital One* case, the nature surrounding the dissemination of the report is a significant factor in determining whether the report remains protected. As a result, counsel

may want to consider tightly controlling and limiting the distribution of the reports, including the sharing of the privileged report with unnecessary leadership (*e.g.*, leadership in IT, Security, Communications, etc.). If security and technical recommendations are needed, then consider reserving those for an oral read-out or separate written summary.

The most difficult distribution decision for companies and counsel will be selecting what to share with regulatory authorities and law enforcement. The recent unfavorable view by courts with the sharing of privileged information and reports with regulatory authorities and law enforcement means counsel should strongly consider avoiding instinctively turning over these reports to such entities. Instead, they may want to look closely at their regulatory obligations and only share that information that is explicitly required by law or regulation.

Conclusion

For counsel, maintaining privilege during a fast-moving incident with high operational risk has always been a difficult task. However, in light of recent court decisions, that task has become even more difficult. Despite the increased odds, counsel can take deliberate steps, like those outlined above, to prepare their clients for this challenge.

About the Author

Griffin Weaver is senior cybersecurity counsel at Dell Technologies, and an adjunct professor at a university where he teaches a Cybersecurity Law class for cybersecurity professionals pursuing their masters degree.

He has authored and coauthored several articles covering a variety of cybersecurity related topics. He has also presented at a number of cybersecurity focused conferences.

Griffin lives in San Antonio Texas with his better half and two rambunctious children.

Prior to beginning his legal career, he worked in the IT field holding a number of different technical and managerial positions. He attended law school at the University of Utah and has worked in a number of highly regulated industries since then.

Downloading Liability? The Evolving Trend of Product Liability Exposure for Apps

By John G. Browning

Consumer applications—"apps"—are big business. This year—barely ten years since the iPhone App Store and Google Play store first launched—mobile app downloads are expected to reach 258 billion.[1] That's a 45% increase since 2017. By 2022, the industry is projected to generate over $156 billion in consumer app spending.[2] U.S. consumers are using their smartphones more than watching television, and 70% of the time spent on digital media is completed in an app. These trends show no sign of slowing down; in fact, since the pandemic began, mobile app downloads have grown 23.3%.[3] But with this increased reliance has come another evolution—a growing trend among courts in viewing apps not as a connection between consumers and service providers, but as end products being delivered to consumers. As a result, software designers, hardware manufacturers, and their insurers now have to consider the very real prospect of product liability litigation and legal responsibility for the indirect injuries and distractions that apps can cause.

I. IN THE BEGINNING

Perhaps the first serious discussions about product liability exposure for apps began with the unprecedented popularity of, and widespread publicity about, the Pokémon GO app in 2016. With its location-based augmented reality (AR) experience, the Pokémon app raised novel legal questions about users' legal interactions with the world and property laws. There were countless media reports about the craze, including how Pokémon GO players were so caught up in the game that they walked into hazardous situations, trespassed onto private property, or even became the victim of violent crime when they failed to see an attack coming. In 2019, developer Niantic settled a class action lawsuit stemming from the nuisance claims of property owners who lived near the real world locations converted into the game's Pokéstops.[4] And

---

1 Liam Burns, *8 Stats You Need to Know About Mobile Apps in 2021*, WWW.DECIBEL.COM (Dec. 17, 2020), https://decibel.com/blog/8-stats-you-need-to-know-about-mobile-apps-in-2021 (last visited Jun. 18, 2021).

2 *Id.*

3 *Id.*

4 Alissa McAloon, *Niantic Settles Pokémon Go Public Nuisance Class Action Lawsuit*, WWW.GAMASUTRA.COM (Sept. 5, 2019), https://www.gamasutra.com/view/news/350223/Niantic_settles_Pokemon_Go_public_nuisance_class_action_lawsuit.php (last visited Jun. 18, 2021).

while Pokémon GO provided users with a variety of pop-up warnings about the risk of physical injury associated with its activities (and also included an express limitation of liability in its Terms and Conditions), that did not prevent Niantic from being sued all over the country, including over major injuries in New York, California, and Pennsylvania.[5] In addition, traditional product liability defenses like assumption of the risk were of limited value, since they varied in effect from state to state (for example, in comparative fault states like Texas, Florida, and California, assumption of the risk would not necessarily operate as a complete bar). Despite this, Niantic managed to fend off the legal assaults over its virtual creatures, and the appellate courts were not presented with the opportunity to consider the strict liability ramifications of the popular Pokémon GO app.

II. HEALTH APPS

Another potential dimension for apps' product liability exposure came from one of the largest markets within the app community: fitness, wellness, and medical apps. Consumers use these apps for everything from tracking weight and blood pressure to gathering personal health information and sharing it with doctors. But mobile medical apps (MMAs) pose unique concerns, in that the Food & Drug Administration stepped in in 2015 with its Final Guidance on MMAs, pronouncing such mobile apps as medical devices, and therefore subject to FDA regulations. This regulatory oversight specifically targets medical apps that function as medical instruments, such as those that are connected to and control devices like blood pressure machines or insulin pumps. Apps that help track a consumer's medical data, but do not provide specific treatment suggestions or connect to wired devices, are deemed to be lesser risks and therefore not subject to FDA regulations.

These changes in the regulatory landscape for digital health products were hastened by federal legislation. In Section 3060 of the 21st Century Cures Act, Congress amended the definition of "device" to exclude certain software functions. It provides that when a medical device has multiple functions (such as both device and non-device software functions), then the FDA is not permitted to regulate the non-device functions. Yet the nature of digital health products can make the question of assessing liability a difficult one. Some digital health products are a system of connected parts, with different parts subject to different standards. A device will be subject to FDA oversight, while an app associated with it may or may not, depending on whether it has device functions under the Cures Act. To add to the potential confusion, there

---

[5] Celina Kirchner, *Guest Post: Pokémon Oh No! Augmented Reality Raises Specter of Personal Injury Claims*, GEEKWIRE (Aug. 6, 2016), https://www.geekwire.com/2016/guest-post-pokemon-oh-no-augmented-reality-raises-specter-personal-injury-claims/ (last visited Jun. 18, 2021).

may also be third parties supporting the app's functions, like a data analytics firm that analyzes the device's raw data and provides feedback.

Against this backdrop is the central question that this article poses—is the MMA's software a "product" or a "service"? Under the Restatement (Third) of Torts, a product is defined as "tangible personal property distributed commercially for use or consumption."[6] Nationally, courts have reached conflicting holdings about whether software can be regarded as a tangible product. Other thorny issues can hinge on the "product" question as it regards mobile medical apps, including jurisdiction. In the wake of recent U.S. Supreme Court decisions involving personal jurisdiction,[7] it could become difficult to determine whether a medical product manufacturer may be subject to jurisdiction in a forum other than its home state, such as the forum where the app developer resides. A number of factors become part of this equation, such as the degree of control and oversight the medical manufacturer has over the design of the connecting app and how integrated the app is to the overall product functioning.

III. EARLY FAILURES IN "BLAMING THE APP"

A. Herrick v. Grindr

Should an app enjoy the same immunity from civil liability under Section 230 of the Communications Decency Act? That question has been posed repeatedly, with little success. In 2015, Matthew Herrick met his boyfriend through the social app Grindr. The couple broke up in 2016, and shortly thereafter a wave of abuse began directed against Herrick by his ex, identified only as J.C. Between October 2016 and March 2017, over 1,000 men came to Herrick's home and his workplace, believing that Herrick had invited them there for violent sex, including rape fantasies. Herrick had no idea who these men were and had never communicated with them. The men, on the other hand, swore that they had "matched" with Herrick and conversed with him on apps like Grindr. As it turns out, Herrick's vindictive ex-boyfriend had created false profiles and impersonated Herrick online. Herrick filed criminal complaints and sought protective orders against J.C., but that did little to deter the unwanted activity.

Herrick also made over 100 complaints to Grindr. When the company failed to take action, he sued it. Herrick's lawsuit alleged product liability complaints, arguing that Grindr is a defectively designed and manufactured product that lacked the ability to identify and exclude

---

6 Restatement (Third) of Torts: Prod. Liab. § 19 (1998).

7 *Bristol-Myers Squibb Co. v. Superior Court of California*, 582 U.S. ___, 37 S.Ct. 1773 (2017).

abusive users. Grindr responded by removing the case from New York state court in 2018 to federal court, and arguing that it was immune from liability pursuant to Section 230. In January 2019, the New York federal judge ruled in Grindr's favor. Herrick appealed, but on March 27, 2019, the Second Circuit affirmed the lower court's dismissal of the case. An appeal to the U.S. Supreme Court followed, but in October 2019, the Supreme Court refused to grant certiorari.[8]

B. Beckman v. Match.com

A similar lawsuit alleging product liability claims against another dating app fared no better before the Ninth Circuit. In *Beckman v. Match.com*, Mary Kay Beckman alleged that she had been "matched" with another user on the defendant's site and app, only to have that user viciously attack her.[9] Beckman asserted negligence and product liability causes of action, including a failure to warn claim under Nevada law. However, both the trial court and the Ninth Circuit were unconvinced by Beckman's allegations and summarily dismissed her case. The main holding was that Beckman was not in a "special relationship" with Match, such that it would have owed her a duty (such as landowner-invitee, or hospital-patient). In the absence of such a relationship, the Ninth Circuit affirmed there could be no duty to warn.[10]

IV. SNAPCHAT AND THE TURNING OF THE TIDE

More recent efforts to hold app developers strictly liable as the makers of a defective product have fared only slightly better, due to the wildly popular app Snapchat. What's particularly at issue is the app's "speed filter" issue that tracks how fast someone is traveling while they take a selfie that memorializes the speed. Because Snapchat photos and videos disappear after viewing, personal injury attorneys maintain that they demand even more concentration, resulting in higher risk of distracted driving.

A. Maynard v. Snapchat

In April 2015, then 18 year-old Christal McGee was driving her father's Mercedes C230 at over 100 miles per hour with three passengers in her car, when she slammed into Wentworth Maynard's Mitsubishi Outlander.[11] The impact knocked Maynard into a highway barrier, causing severe personal injuries, including brain injury. Maynard's lawsuit claimed that McGee was driving at an excessive rate of speed as she attempted to reach 100 mph and capture that

---

[8] Carrie Goldberg, Herrick v. Grindr*: Why Section 230 of the Communications Decency Act Must Be Fixed*, www.LAWFARE.COM (Aug. 14, 2019), https://www.lawfareblog.com/herrick-v-grindr-why-section-230-communications-decency-act-must-be-fixed, (last visited Jun. 18, 2021).

[9] *Beckman v. Match*, 743 Fed. Appx. 142, No. 17-16043 (9th Cir. Nov. 21, 2018).

[10] *Id.*

[11] *Maynard v. Snapchat, Inc.*, 357 Ga. App. 496. 2020 WL 6375424 (Ga. Ct. App. Oct. 30, 2020).

speed on a selfie using the Speed Filter. Maynard further alleged that Snapchat's feature was defectively designed, since it encouraged users to endanger themselves and others while on the roadway. Maynard argued that Snapchat had violated Georgia product liability law, which imposes a duty on manufacturers "to exercise reasonable care in manufacturing its products to make products that are reasonably safe for intended or foreseeable users."[12]

Snapchat responded with an argument that it was immune from liability under Section 230. The trial court agreed, dismissing the case. On appeal, the Georgia Court of Appeals reversed, holding that Section 230 didn't apply to the speed filter. It sent the case back to the trial court to review the case on the merits. This time, focusing on the product liability argument, the trial court again ruled in Snapchat's favor, holding that Snapchat "had no duty to alter the design of its mobile application to prevent McGee from driving recklessly or negligently."[13] Once again, Maynard appealed.

In a 2-1 decision, the Georgia Court of Appeals affirmed the dismissal, holding that the allegedly negligent design claim does not fall within Snapchat's duty of care to the plaintiff. It noted that Georgia law does not impose a general duty to prevent people from committing torts while misusing a manufacturer's product. While manufacturers may have a duty to exercise reasonable care in manufacturing products that are reasonably safe for intended or foreseeable users, the Court reasoned, "this duty does not extend to the intentional (not accidental) misuse of the product in a tortious way by a third party."[14] The dissent argued that—employing a risk/utility balancing test—the plaintiff had made a sufficient argument of design defect and demonstrated Snapchat owed a duty to design the product differently so as to avoid accidents like the one in question.[15]

B. Lemmon v. Snap, Inc.

Even more recently, the 9th Circuit similarly rejected Snapchat's Section 230 immunity defense. In *Lemmon v. Snap, Inc.*, the surviving parents of two of three boys killed in a high speed car accident in Wisconsin sued the app developer.[16] Shortly before running off the road on May 28, 2017, one of the young men had opened Snapchat to document the 113 mph speed at which they were traveling. The Speed Filter, superimposed over the photos or video, enabled them to

---

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *See id.* (McFadden, C.J., dissenting).

[16] *Lemmon v. Snap, Inc.*, 2021 U.S. App. LEXIS 13197, No. 20-55295 (9th Cir. May 4, 2021).

"record their real-life speed."[17] The trial court dismissed the case, ruling that Snapchat was immune from liability under Section 230.

On appeal, the 9th Circuit reversed. It rejected the applicability of Section 230, and stated that the plaintiffs' claims did not involve Snapchat's role as a publisher, but as a designer:

> [T]he duty that Snap allegedly violated "springs from" its distinct capacity as a product designer. . . . Snap indisputably designed Snapchat's reward system and Speed filter and made those aspects of Snapchat available to users through the internet. . . . And the Parents' negligent design claim faults Snap solely for Snapchat's architecture, contending that the app's Speed Filter and reward system worked together to encourage users to drive at dangerous speeds.

The 9th Circuit panel remanded the case, and so the product liability theory will proceed to trial.

V. CONCLUSION – WHAT DOES THE FUTURE HOLD?

Certainly, the trend seems to be moving away from Section 230 immunity providing a "get out of jail free" card for app developers when it comes to product liability claims. This may result in an uptick in product liability litigation being pursued against apps for torts resulting from their use by third parties. For example, Snap was sued in May in federal court in the Northern District of California by the estate of Carson Bride. Bride was a 16 year-old who took his own life after being the victim of cyberbullying, in which the use of apps like Snapchat, YOLO, and LMK (all anonymous messaging apps popular with teenagers) were extensively used by his tormentors. The lawsuit includes strict liability causes of action, contending that the anonymous messaging functionality of the apps was a design, and its misuse by cyberbullies was reasonably foreseeable.

And if an app can be considered a "product," why not an algorithm? After 26 year-old Christian Rodgers was murdered by a convicted felon on parole, his mother, June, sued the makers of the algorithm used in assessing the felon's suitability for parole.[18] The felon, Jules Black, had been arrested on April 5, 2017, by New Jersey State Police and was charged with being a felon in possession of a firearm. Black had been released on non-monetary conditions the next day because he had a low Public Safety Assessment (PSA) score, per the defendant's algorithm; on

---

[17] *Id.*

[18] *Rodgers v. Laura & John Arnold Found.*, 2019 WL 2429574 (D.N.J. June 11, 2019).

April 9, Black murdered Rodgers. Mrs. Rodgers brought suit under the New Jersey Products Liability Act, arguing that the algorithm was a defective product.[19]

The court, however, disagreed and dismissed Rodgers' suit. It held that the PSA was not a "product" within the meaning of New Jersey's statute. Moreover, the judge reasoned the algorithm itself is "neither a tangible product or a non-tangible 'other item' as contemplated by section 19 of the Restatement of Torts and it is not distributed commercially."[20] Ruling that the PSA "constitutes information, guidance, ideas, and recommendations as to how to consider the risk a given criminal defendant presents," the court reasoned that the PSA could not be subject to strict liability since it was properly treated "as speech, rather than product."[21]

Ultimately, the analysis of whether an app is considered a "product" or not will revolve around questions unique to a given state's products liability statute. Just as an e-commerce platform like Amazon can be considered as the "seller" of a defectively-designed product that it did not design, manufacture, or market depending on which state's law applies, similar confusion may reign when an app is involved.

About the Author

John Browning is a former Justice on Texas' Fifth Court of Appeals, immediate past chair of the Computer and Technology Section of the State Bar, and a partner in the Plano office of Spencer Fane LLP.

[19] *Id.*
[20] *Id.*
[21] *Id.*

Steganography: Because Who Doesn't Love Bacon?

By Craig Ball

Updating my E-Discovery Workbook to begin a new semester at the University of Texas School of Law, and I can't help working in historical tidbits celebrating the antecedents of modern information technology. Digital encoding is a topic I regard as essential to a good grasp of digital forensics and electronic evidence. When you understand encoding, you understand why varying sources of electronically stored information are more alike than different and why forms of production matter.

We record information every day using 26 symbols called "the alphabet," abetted by helpful signals called "punctuation." So, you could say that we write in hexavigesimal (Base26) encoding.

"Binary" or Base2 encoding is notating information using nothing but two symbols: conventionally, the numbers one and zero. It is often said that "computer data is stored as ones and zeroes;" but that's a fiction. In fact, binary data is stored physically, electronically, magnetically or optically using mechanisms that permit the detection of two clearly distinguishable "states," whether manifested as faint voltage potentials (*e.g.,* thumb drives), polar magnetic reversals (*e.g.,* spinning hard drives) or pits on a reflective disc deflecting a laser beam (*e.g.,* DVDs). Ones and zeroes are simply a useful way to *notate* those states. You could use *any* two symbols as binary characters, *or even two discrete characteristics of the "same" symbol.* For now, just ponder how *you* might record or communicate two "different" characteristics, as by two different shapes, colors, sizes, orientations, markings, etc.

I free you from the trope of ones and zeroes to plumb the evolution of binary communication and explore an obscure coding cul-de-sac called **Steganography**, from the Greek, meaning "concealed writing." But first, we need an aside of Bacon.

I mean, of course, lawyer and statesman **Sir Francis Bacon** (1561-1626). Among his many accomplishments, Bacon conceived a bilateral **cipher** (a "code" in modern parlance) enabling the hiding of messages *omnia per omnia,* or "anything by anything."

Bacon's cipher used the letters "A" and "B" to denote binary values; but if we use ones and zeros instead, we see the straight line from Bacon's clever cipher to modern ASCII and Unicode encoding.

As with modern computer encoding, we need multiple binary digits ("bits") to encode or "stand in for" the letters of the alphabet. Bacon chose the five-bit sets at right:

If we substitute ones and zeroes (right), Bacon's cipher starts to look uncannily like contemporary binary encodings.

Why *five* bits and not three or four? The answer lies in binary math ("*Oh no! Not MATH!!*"). Wait, *wait*; it won't hurt. I promise!

Letter	Code
A	AAAAA
B	AAAAB
C	AAABA
D	AAABB
E	AABAA
F	AABAB
G	AABBA
H	AABBB

Letter	Code
I/J	ABAAA
K	ABAAB
L	ABABA
M	ABABB
N	ABAAB
O	ABABA
P	ABBBA
Q	ABBBB

Letter	Code
R	BAAAA
S	BAAAB
T	BAABA
U/V	BAABB
W	BABAA
X	BABAB
Y	BABBA
Z	BABBB

Letter	Code
A	00000
B	00001
C	00010
D	00011
E	00100
F	00101
G	00110
H	00111

Letter	Code
I/J	01000
K	01001
L	01010
M	01011
N	01100
O	01101
P	01110
Q	01111

Letter	Code
R	10000
S	10001
T	10010
U/V	10011
W	10100
X	10101
Y	10110
Z	10111

If you have one binary digit (2^1), you have only two unique states (one or zero), so you can only encode two letters, say A and B. If you have two binary digits (2^2 or 2×2), you can encode four letters, say A, B, C and D. With three binary digits (2^3 or 2x2x2), you can encode eight letters. Finally, with four binary digits (2^4 or 2x2x2x2), you can encode just sixteen letters. *So, do you see the problem in trying to encode the letters of a 26-letter alphabet?* You must use at least five binary digits (2^5 or 32) unless you are content to forgo ten letters.

Sir Francis Bacon was not especially interested in encoding text as bits. His goal was to *hide* messages in any medium, permitting a clued-in reader to distinguish between differences lurking in plain sight. Those differences—whatever they might be—serve to denote the "A" or "B" in Bacon's steganographic technique. For example:

I hi**d** m**y** name in this **s**enten**c**e as a se**r**ies of b**o**l**d**ed **l**et**t**ers.

I hi*d* m*y* name in this *s*enten*c*e as ita*l*icized *c*ha*r*ac*t*ers.

I hid my name in this sentence as sans serif characters.

That last one is quite subtle, right? Here's how it's done:

Using Bacon's cipher, CRAIG BALL is AAABA BAAAA AAAAA ABAAA AABBA AAAAB AAAAA ABABA ABABA
C R A I G B A L L

To conceal my name in each of the respective examples, every unbolded/unitalicized/serif character signifies an "A" in Bacon's cipher and every boldface/italicized/sans serif character signifies a "B" (ignore the spaces and punctuation).

sans

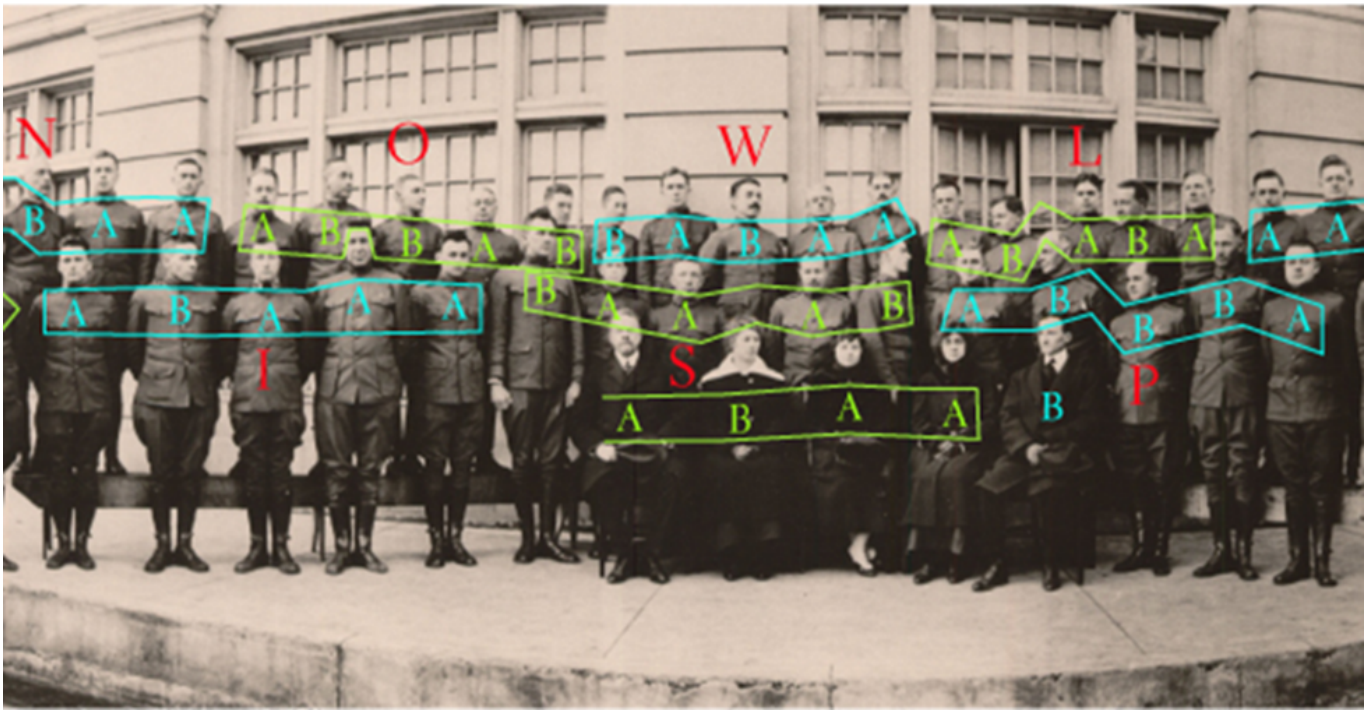
The bold and italic approaches look wonky and could arouse suspicion, but if the fonts are chosen carefully, the absence of serifs should go unnoticed. Take a closer look to see how it works:

I hid my name in this sentence as sans serif characters.
A AAB AB AAAA AA AAAA BAAAAABB AA AAAB AAAAA ABABAABABA.

In my examples, I have used Bacon's cipher to hide text within text, but it can as easily hide messages in almost anything. My favorite example is the class photo of World War I cryptographers trained in Aurora, Illinois by famed cryptographers, William and Elizabeth Friedman.[1] Before they headed for France, the newly minted codebreakers lined up for the cameraman; but there is more going on here than meets the eye.

Taking to heart *omnia per omnia*, the Friedmans ingenuously encoded Sir Francis Bacon's maxim "knowledge is power" within the photograph using Bacon's cipher. The 71 soldiers and their instructors convey the cipher text by facing or looking away from the camera. Those facing denote an "A." Those looking away denote a "B." There were not quite enough present to encode the entire maxim, so the decoded message actually reads, "KNOWLEDGE IS POWE." Here's the decoding:

A closer look:



Isn't that mind blowing?!?!

Steganography is something most computer forensic examiners study but rarely use in practice. Still, it is a fascinating discipline with a history reaching back to ancient Greece, where masters tattooed secret messages on servants' shaved scalps and hit "Send" once the hair grew back. Digital technology brought new and difficult-to-decipher steganographic techniques enabling images, sound and messages to hitch a hidden ride on a wide range of electronic media.

For this material, I'm indebted to "How to Make Anything Signify Anything" by William H. Sherman in Cabinet no. 40 (Winter 2010-2011).

About the Author

Craig Ball teaches Electronic Evidence at the University of Texas and Tulane University Schools of Law. He limits his practice to service as a Special Master in eDiscovery and Computer Forensics.

Drone Surveillance Requires a Warrant

By Pierre Grosdidier

No one likes to see a drone hovering over one's property, especially when such aerial antics are unauthorized. Long Lake Township in Michigan used a drone to confirm that Maxon operated an illegal salvage or junk yard on his property, which was hidden from view from the roadside.[1] The township sued Maxon, who moved to suppress the drone photo evidence because neither he nor a court had greenlighted the overflights. Maxon argued that the flights amounted to an illegal search in violation of the Fourth Amendment. The trial court denied Maxon's motion, but the Michigan Court of Appeals reversed. The case is important because it differentiates low-altitude drone flights from airplane and helicopter overflights in the navigable airspace, which the U.S. Supreme Court has long held are legal.

The Fourth Amendment protects persons from unreasonable searches. The search of a home and its curtilage, its immediate surrounding, requires a warrant supported by probable cause, with exceptions.[2] A Fourth Amendment search also occurs when authorities intrude on a person's subjective expectation of privacy that society recognizes as reasonable. In analyzing the person's expectation, the court must consider "the totality of the circumstances surrounding the intrusion."[3] For example, a person in a phone booth can reasonably expect to conduct a phone conversation without being recorded unless the police have a search warrant.[4] But, what a person knowingly exposes to the public enjoys no Fourth Amendment protection.[5] Thus, the police's plain visual observation of a house from a public thoroughfare is not a search.

The parties in this dispute had met in the courtroom before. A decade earlier, they had litigated and settled a similar dispute. The township sued again in 2018 and introduced drone photos showing the allegedly expanding junk yard. Maxon argued that the pictures violated his

---

1 *Long Lake Twp. v. Maxon*, --- N.W.2d ---, 2021 WL 1047366, No. 349230, at *1 (Mich. Ct. App. Mar. 18, 2021). A private subcontractor performed the drone flights acting for the township. *Id.* at *3.

2 *Id.* at *3.

3 *Id.* at *8.

4 *Katz v. United States*, 389 U.S. 347 (1967).

5 *Maxon*, 2021 WL 1047366, at *8.

subjective reasonable expectation of privacy and that the drone's flight violated FAA regulations, an allegation that the drone's operator rejected. In denying Maxon's motion to suppress, the trial court relied on *Florida v. Riley*, a U.S. Supreme Court case that held that a landowner does not have a subjective reasonable expectation of privacy from a police helicopter overflight 400 feet above his property.[6] *Riley* stands for the proposition that the Fourth Amendment does not bar the police from observing the inside of a greenhouse from a public vantage point where they have a right to be, be it from an airplane or a helicopter in the navigable airspace.

The *Maxon* court first reiterated the U.S. Supreme Court's position in *Kyllo v. United States* that what society and the law are willing to recognize as a reasonable expectation of privacy is not a moving target that recedes with improving surveillance technology.[7] In *Kyllo*, the U.S. Supreme Court held that thermal imaging of a home from a public vantage point was a Fourth Amendment search that required a warrant. The Michigan Court of Appeals also drew on *Riley* and its dissenting opinions to reject Maxon's argument that noncompliance with FAA regulations was tantamount to a violation of the Fourth Amendment.[8] What counts "is not whether the police were where they had a right to be under FAA regulations," but whether a person's expectation of privacy was "rendered illusory" by possible public observation from aerial traffic in the navigable airspace.[9] In *Riley*, the U.S. Supreme Court confirmed that such expectation was illusory because these overflights were nonintrusive and anyone flying a plane could look down and see what the police saw inside the greenhouse.[10]

In this case, inspired by *Kyllo*, the court concluded that "low-altitude, unmanned, specifically-targeted drone surveillance of a private individual's property is qualitatively different from the kinds of human-operated overflights permitted by *Ciraolo* and *Riley*."[11] It held that such flights encroached on a person's reasonable expectation of privacy and, therefore, required a Fourth Amendment search warrant, or an exception thereto such as consent.[12] Drones, the court observed, are more intrusive than airplane overflights; they are less frequent, inadvertent, and

---

6 *Id*. at *4 (citing *Florida v. Riley*, 488 U.S. 445 (1989)).

7 *Id.* at *8 (citing *Carpenter v. United States*, 138 S. Ct. 2206, 2217–19 (2018); *Kyllo v. United States*, 533 U.S. 27, 33–35 (2001).

8 *Id*. at *17.

9 *Id.*

10 *Id*. at **14–15 (citing *California v. Ciraolo*, 476 U.S. 207, 212–15 (1986).

11 *Id*. at *18–19.

12 *Id*. at *19; n.4.

costly, and inherently much easier to deploy. Moreover, drones' agility, speed, and stealth drastically expand their surveillance abilities "not just in degree, but in kind." Significantly, the court saw "little meaningful distinction" in this case between drone flights just inside and outside a property line.[13] The key issue remained a person's reasonable expectation of privacy, which included the expectation that a drone overflight would be exceptional and trespassory, regardless of whether the drone flew at 300 feet or directly against a bathroom window.

Separately, the court declined to decide whether these drone flights constituted a physical trespass, because the question was not dispositive. The U.S. Supreme Court has held that landowners retain some ownership of the space above their property, even if that ownership no longer extends to the heavens as under the common law.[14] The Michigan Court of Appeals observed that because drones fly below the navigable airspace, their unauthorized or nonpermissive acrobatics over private property might reasonably be considered trespassory. But, the court noted, the issue is not necessarily tied to the Fourth Amendment because a drone flight over a field might constitute a trespass, but not a Fourth Amendment search.

About the Author

Pierre Grosdidier is an attorney in Houston. 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), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Treasurer for 2020–21.

[13] *Id.* at *21.

[14] *Id.* (citing *United States v. Causby*, 328 U.S. 256, 260–65 (1946)).

Fit to Admit – The Latest on New Sources of Digital Evidence

By John G. Browning

As many readers may know, I have previously chronicled new sources of digital evidence—from sources like fitness trackers, health apps, and other denizens from the Internet of Things (IoT)—in other articles like *Fit to Admit* in the *Texas Bar Journal*. But with this area of evidence continually expanding as the IoT grows (the number of web-enabled devices nearly tripled from 13.4 billion in 2015 to 38.5 billion in 2020), new examples continue to populate our legal system.

Consider doorbell cameras like Amazon's Ring, for example. Digital evidence from such devices is beginning to regularly crop up in court. In January 2020, a Ring doorbell camera apparently captured audio of former UT-San Antonio football star Michael Egwuagu allegedly confessing to the stabbing death of his pregnant sister (he was later found not guilty by reason of insanity). Another Texas case dealt with authentication of such evidence. In *Chatman v. State*, a home invasion case, the victim was at home when he received a notification on his cell through the Ring app; he answered the door and was violently assaulted.[1] Portions of the assault and its aftermath were captured in three videoclips, which were downloaded by the victim and emailed to law enforcement.

At trial, the defense objected on multiple grounds, including insufficient authentication. The trial court overruled, and the defendant was convicted. The 5th Court of Appeals affirmed, holding that the victim was a witness with personal knowledge who observed the scene and that the Ring video evidence was properly authenticated through his testimony.[2] Evidence from Ring devices have proved pivotal in other cases around the country as well, including a 2020 shooting case in Rochester, New Hampshire and a 2020 appellate decision in Utah arising out of a burglary case.[3]

Health apps and fitness trackers are also becoming increasingly important as sources of evidence. Earlier this year, Jeff West of Alabama was sentenced to 16 years in prison for the reckless manslaughter of his wife. Among the factors leading to his conviction was his alibi being contradicted by data from his phone's health app. West had told police that he was asleep at 10:30 p.m. on the night of his wife's 2018 death. However, his health app revealed

---

1 *Chatman v. State*, 2018 Tex. App. LEXIS 10597, 2018 WL 6629531 (Tex. App.—Dallas 2018).

2 *Id.* at *17.

3 *See State v. Rogers*, 2020 UT App. 78, 467 P.3d 880 (May 21,2020).

that West took 18 steps between 11:03 p.m. and 11:10 p.m. (there was other evidence that indicated the wife had been killed not by a fall, but by a blow to the head).

A recent case illustrates that courts are growing more aware of the importance of these new sources of digital evidence. Guan Hollins sued Zimmer Biomet Holdings, a maker of artificial hips, in 2015, claiming that the artificial hip that he'd had implanted in 2007 was defective, and was causing him to experience pain and lack of mobility. Hollins had surgery in 2015 to remove the artificial hip and began wearing a Fitbit several months later. After Hollins disclosed this in an interrogatory, the defense sought electronically stored information from the device. They reasoned that data indicating that Hollins was walking or running miles every day was relevant to his claims of permanent injury. Hollins countered that this objected to a fishing expedition.

U.S. District Judge John Ross of the Eastern District of Missouri agreed with the defense, and in a May 24, 2021 order, ruled that Hollins must turn over data from his Fitbit.[4] Judge Ross pointed to the relevance, the "extremely low burden of production," and the limited privacy risks involved.[5] However, he did allow Hollins to redact any information concerning his heart rate, sleep records, or physical location since such information was irrelevant. Judge Ross expressed surprise that there was "surprisingly little precedent on this issue given the ubiquitous presence of wearable devices."[6] Interestingly, one of the few cases that the court cited was a Texas personal injury case, *Cory v. George Carden International Circus*. In *Cory*, Judge Ron Clark found that "a mobile app that indicates a Plaintiff performs strenuous activities may be relevant to claims of injury or disability."[7]

Regardless of whether you are on the side of the plaintiff or the defendant, the prosecution or the defense, data from such relatively new sources of digital evidence is playing an increasingly pivotal role in cases. Counsel needs to be cognizant of everything that might be "fit" to admit, including fitness trackers and other items from the Internet of Things.

---

4 *Barts v. Biomet, Inc.*, No. 4:13-CV-00657-JAR (E.D. Mo. May 24, 2021).

5 *Id.* at 3.

6 *Id.*

7 *Cory v. George Carden Int'l Circus*, No. 4:13-CV-760, 2016 WL 3460781, slip. op. at 2-3 (E.D. Tex. 2016).

About the Author

John Browning is a former Justice on Texas' Fifth Court of Appeals, immediate past chair of the Computer and Technology Section of the State Bar, and a partner in the Plano office of Spencer Fane LLP.

Obsessed Parents and Technology

By John G. Browning

Here in Texas, we're no strangers to the extent to which parents can become obsessed over their children's extracurricular activities, such as cheerleading, sports, and homecoming. After all, back in 1991, we gave the world Wanda Holloway, the Channelview, Texas "cheerleader mom" who ultimately pled no contest to charges stemming from allegedly hiring a hitman to kill one of her daughter's junior high school cheerleading rivals and her mother. It made headlines all over the world, and even spawned an HBO television movie starring Holly Hunter.

The Digital Age has provided new tools for parents to take their obsession to dangerous new depths. In March, Raffaela Spone of Bucks County, Pennsylvania was charged with multiple counts of harassment arising out of her alleged use of "deepfake" technology to try to get her daughter's cheerleading rivals kicked off the team. Deepfake technology, of course, uses artificial intelligence to digitally manipulate photos and video. Spone reportedly sent deepfake videos to the cheerleading coach of the competitive squad "The Victory Vipers"—content purportedly showing fellow cheerleaders engaging in prohibited activities like drinking and smoking, as well as depicting them nude. Spone is alleged to have used images from the girls' social media accounts to generate the deepfake images. In addition, she is accused of sending harassing text messages to team members, their parents, and the owners of the cheerleading gym, using fake phone numbers. Authorities traced the phone numbers to a website that sells numbers to telemarketers, and in turn followed the trail to an IP address associated with Spone's home.

The 50 year-old Spone was arrested on March 5 and has been charged with 3 counts of harassment and 3 counts of cyberharassment of a child. The deepfake images were sent to her daughter's teen rivals from an anonymous account accompanied by messages urging the girls to kill themselves. Spone is free on bail.

And if you thought only presidential elections would face concerns about cyberintrusion and election integrity, then you may underestimate the lengths to which a "helicopter parent" will go. In March 2021, Laura Rose Caroll and her now 18 year-old daughter, Emily Grover, were arrested for allegedly hacking into people's online accounts and submitting 250 fake votes to interfere in the race for homecoming queen of Tate High School in Pensacola, Florida. Ms. Caroll, who works as the assistant principal of a nearby elementary school, allegedly used her school district account to open 372 student records—339 of whom attended Tate. The Florida

Department of Law Enforcement initiated a month-long investigation last November, after the school district reported fraudulent access to student profiles. The investigation revealed that 117 votes were cast from the same IP address over a very brief window of time. It also showed that 246 votes were placed from accounts accessed from computers inside the mother and daughter's home, or from Ms. Caroll's cellphone. In fact, some of Ms. Grover's classmates said she had bragged about voting from her mother's school district account.

Both defendants, who are free on bail, have been charged with offenses against users of computers and computer systems, unlawful use of a two-way communications device, criminal use of personally identifiable information, and conspiracy. Sadly, while harassment of their kids' rivals and vote-rigging are extremes that obsessed parents have stooped to for years, today's technology has afforded them dangerous new tools.

About the Author

John Browning is a former Justice on Texas' Fifth Court of Appeals, immediate past chair of the Computer and Technology Section of the State Bar, and a partner in the Plano office of Spencer Fane LLP.

Technology for Disaster-Proofing Your Practice

By John G. Browning

Lawyers and law firms throughout Texas are no strangers to the challenge of coping with natural disasters. From Hurricane Harvey in 2017 to the statewide power outages of February's "Icepocalypse," we have survived regular reminders from Mother Nature of how severe weather can threaten lives and impact business continuity. And while there are many resources to consider when it comes to disaster preparedness, having a plan is paramount and technology should be near the top of your list. In fact, according to the International Legal Technology Association (ILTA) 2020 Legal Technology Survey, 75% of responding lawyers indicated that their firms have disaster plans in place; another 22% responded that they were working on such a disaster plan.

Preparing and adopting a disaster recovery plan is a top priority. Even a solo or small firm practice should have a comprehensive plan that covers everything from data protection, employee contingencies, safety and first aid, communication options, and maintaining the confidentiality of your client communications. If you are unsure what to address in your disaster plan, there are helpful resources to consult, including the ABA's guide "Surviving a Disaster: A Lawyer's Guide to Disaster Planning" (prepared by the ABA Special Committee on Disaster Response and Preparedness, and accessible along with other resources at www.americanbar.org/disaster). This guide addresses issues like alternate facilities, communications continuity, and vital records management. Another handy resource for planning ahead is the "Disaster Planning and Recovery" guide prepared by Lawyers Mutual Insurance Company, which includes some sample forms and checklists. Ideally, your plan should address who in your firm is responsible for critical tasks like emergency communications and IT data safety and recovery, and it should include cross-designations—just in case some people have lost communications or are physically prevented from performing their designated emergency preparedness task. If possible, always have a backup ready to step in.

Planning ahead and addressing the technology needed to help you cope in the event of a natural disaster is not just a practical necessity—it is an ethical imperative as well. In September 2018, the ABA Standing Committee on Ethics and Professional Responsibility issued

Formal Ethics Opinion 482, entitled "Ethical Obligations Related to Disasters."[1] In it, the ABA examined a number of topics, including practice by lawyers displaced by a disaster and lawyer advertising directed to disaster victims. But it also reminded lawyers of their duty under Rule 1.1 (Texas Rule 1.01) to develop sufficient competence in technology to meet their ethical obligations after a disaster. These other ethical duties include our obligations to communicate with clients and to safeguard client property (including data) and funds. For the former, Opinion 482 reminds lawyers to:[2]

> evaluate in advance storing files electronically so that they will have access to those files via the Internet if they have access to a working computer or smart device after a disaster. If Internet access to files is provided through a cloud service, the lawyer should (i) choose a reputable company, and (ii) take reasonable steps to ensure that the confidentiality of client information is preserved, and that the information is readily accessible to the lawyer.

So besides formulating a disaster plan and being aware of your ethical obligations, what other technology-related steps should you take to get your practice through a natural disaster? First, if you are not already making use of cloud-based solutions to backup and store data, you should consider using them. Onsite backup on network attached storage (NAS) or a storage area network (SAN) may allow you to recover data more quickly because the local backup is in the same place as your original device, but unlike offsite backup in the cloud, it is vulnerable to natural disasters. There are many cloud-based options to store data and documents, including Carbonite, Google Drive, iCloud, One Drive, Dropbox, and more. Second, besides storing data in the cloud, you may wish to consider cloud-based practice management solutions, enabling you to not only access your data once you have an internet connection, but also to keep track of your calendar, court deadlines, document management and integration, timekeeping, and so on. There are many cloud-based practice management solutions out there that are user-friendly, including Clio, Rocket Matter, Amicus Attorney, and others.

What about email? Before disaster strikes, make sure you have an email service vendor that "spools" (retains) your email for delivery when power is restored or—even better—synchronizes with your mailbox and provides an alternate mail transport mechanism. Some vendors will not

---

[1] Formal Ethics Opinion 482, American Bar Association (Sept. 19, 2018), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_482.pdf.

[2] *Id.*

only provide this, but also features like encryption, spam filtering, and phishing prevention. Your service vendor may even be so seamless that your clients will not even know that your primary email technology was down. And be sure to have your system passwords encrypted in the cloud, since you may need them during the recovery phase. Visit with your IT specialist as soon as possible to get a handle on what is functional vs. what is not, and what it will take to get all your systems up and running. And in the event that any of your lawyers and staff have lost laptops, iPads, or other mobile devices in the disaster event itself, be sure that you have the capability to "remote wipe" them to make sure the data on these devices does not fall into the wrong hands. What might have sounded like something out of a spy thriller just years ago is now a standard feature for many law firms, not only on firm-issued laptops but also—thanks to the "Bring Your Own Device" (BYOD) era—on personal devices that an individual attorney owns, such as her iPhone.

There are even more basic concerns if you lose power (like so many did during the "Icepocalypse"). First, you should have surge protectors to protect your computer hardware; a storm surge or even quick flash can corrupt the data on your hard drives, making it impossible to retrieve a document you were working on just minutes before. Combined with cloud-based backup, a surge protector can be a lifesaver. You should also be prepared for power outages by having backup batteries for your computer, so that your practice can keep running even without electricity. Also known as "Uninterruptible Power Supply" (UPS) units, these backup batteries (which often feature built-in surge protectors) are fairly inexpensive (some are as low as $60.00, while others are in the $150.00-$200.00 range). And when the grid goes down, that handy phone charger plugged into your home or office wall is useless. During "Icepocalypse," my alternative was the phone charger that I could plug into my car (my car was our makeshift "warming station" as well). However, to save gas, I recommend having a portable phone charger (already powered up, of course); Zagg, for example, makes one in the $50.00 range. Or you could go "renewable," with a solar-powered phone charger from companies like Anker. In any event, when your phone is your only working lifeline, you need to make sure its power lasts as long as possible. Quick tip: until you can get recharged using your car or a portable power bank, save battery life by turning off Bluetooth, Wi-fi, GPS, and location services—all of which can quickly drain a smartphone's battery.

Finally, if you have devices you can charge, but your home or office internet has gone out, consider using a mobile hotspot or a "Mifi" device (portable broadband) to stay connected to the internet through your wireless cellular network. Handy during the best of times, such

devices can be godsends when the local Starbucks has lost power just like you and the weather conditions make getting out for some “coffee shop Wifi” a dangerous proposition.

In short, you do not have to be MacGyver to keep your practice going during the next natural disaster. But some prior planning when it comes to technology can go a long way.

About the Author

John Browning is a former Justice on Texas’ Fifth Court of Appeals, immediate past chair of the Computer and Technology Section of the State Bar, and a partner in the Plano office of Spencer Fane LLP.

U.S. Supreme Court Narrowly Construes "exceeds authorized access" in the CFAA

By Pierre Grosdidier

In a long-awaited decision, the U.S. Supreme Court resolved a Circuit split and narrowly construed the expression "exceeds authorized access" as defined in the Computer Fraud and Abuse Act ("CFAA").[1] The issue was that of the "rogue insider." Clearly, the CFAA criminalizes breaking into a computer. But, when a person is properly credentialed, does that person exceed their authorized access by obtaining information for illicit reasons? In its 6-3 decision, the U.S. Supreme Court held that the answer is "no."

The F.B.I. caught Georgia police sergeant Van Buren trading information garnered from a law enforcement database for money.[2] Van Buren had credentials to access the database, but clearly not for this reason. He was charged and convicted under the CFAA's § 1030(a)(2), which sanctions whoever "intentionally accesses a computer without authorization or exceeds authorized access."[3] Under the CFAA,[4]

> the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not *entitled so to obtain* or alter.

The Eleventh Circuit, which has construed "exceeds authorized access" broadly, affirmed the CFAA conviction.[5] On appeal to the U.S. Supreme Court, Van Buren argued that the CFAA's "exceeds authorized access" applies only to persons who do not have authorized access to a computer, not to those who misuse this access. The Court agreed.

Sticking closely to the statutory text, the Court accepted Van Buren's argument regarding the importance of the word "so" in the expression "entitled so to obtain." Van Buren clearly

---

1 *Van Buren v. United States*, No. 19-783, --- S. Ct. ---, 2021 WL 2229206 (June 3, 2021); 18 U.S.C. § 1030.

2 *Van Buren*, 2021 WL 2229206, at *1.

3 18 U.S.C. § 1030(a)(2).

4 *Id.* § (e)(6) (emphasis added).

5 *United States v. Van Buren*, 940 F.3d 1192, 1208 (11th Cir. 2019) (citing *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (broad construction of "exceeds authorized access")); compare *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (broad construction), with *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) (narrow construction).

"accessed a computer with authorization" and obtained information. The question was whether he was "entitled *so* to obtain" that information. The Court agreed that "so" is a term of reference that relates to the preceding "identifiable proposition," namely the authorized access to a computer.[6] Under this reasoning, "[t]he phrase 'is not entitled so to obtain' is best read to refer to information that a person is not entitled to obtain by using a computer that he is authorized to access."[7] Thus, a credentialed computer user authorized to access Folder Y does not violate the CFAA by corruptly tapping into this folder, but does exceed authorized access by obtaining information from off-limit Folder X. Authorized access under the CFAA is ultimately a "gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system."[8]

The Court rejected the Government's argument that "so" referred more broadly to "the particular manner or circumstances" in which the user obtained the information.[9] These circumstances, the Government argued, are defined by the terms of access of the information. Under this approach, the Court reasoned, the circumstances that render a person's conduct illicit are not identified in the statute and are potentially overbroad.

The Court also noted that this narrow interpretation of "exceeds authorized access" harmonized the CFAA's §§ (a)(2) and (e)(6), which proscribe accessing a computer without authorization and accessing a computer with authorization and securing information that the user is "not entitled so to obtain." The law, therefore, targets outside hackers and rogue employees who enter areas of the computer that they are not permitted to enter. The CFAA's civil liability provision, the Court added, supports this interpretation. Civil liability depends on a finding of "damage" or "loss," *i.e.*, technological harm such as file corruption, which are typically the consequences of computer hacking, not illicit information retrieval that does not damage a database, as was the case with Van Buren.[10]

The U.S. Supreme Court also dispatched the Government's other arguments. The Government argued that by the plain meaning of words, Van Buren exceeded his authorized access.[11] The

---

6 *Van Buren*, 2021 WL 2229206, at *5-6.

7 *Id*. at *6.

8 *Id*. at *9; *but see id*. n.8 (leaving for another day the issue of whether the gates must be code-based or contractual).

9 *Id*. at *6.

10 *Id*. at *10. And as is also often the case with rogue employees who abscond with their employer's confidential information.

11 *Id*. at *8.

Court countered that what mattered was whether Van Buren did so as defined by the CFAA, not as understood by any ordinary English language speaker. The Government further argued that the original anti-hacking Act clearly targeted rogue employees who accessed information "for purposes to which such authorization does not extend."[12] The Court retorted that the "Government's argument gets things precisely backward." Courts must presume that Congress changes legislation with intent, as it was when it abandoned the statute's reference to "purpose."

The U.S. Supreme Court concluded that a broad construction of "exceeds authorized access" would criminalize the innocuous conduct of "millions of otherwise law-abiding citizens" who use their work-only computers for personal reasons, like checking personal emails, or who stretch the truth on their personal social media pages. This fallout from the Government's broad construction was the "'extra icing on a cake already frosted.'"[13]

About the Author

Pierre Grosdidier is an attorney in Houston. 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), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Treasurer for 2020-21.

[12] *Id*. at *11 (citing 18 U.S.C. § 1030(a)(2) (1982 ed. Supp. III)).
[13] *Id*. (citing *Yates v. United States*, 574 U. S. 528, 557 (2015)).

Texas "Revenge Porn" Law Held Constitutional by Court of Criminal Appeals

By John G. Browning

On May 26, 2021, Texas's highest criminal court upheld the state's 2015 "revenge porn" law, which made it a crime to post intimate photos and video of someone online without that person's consent.[1] In the process, the Court of Criminal Appeals overturned a 2018 decision by the 12th Court of Appeals in Tyler that had found the law unconstitutional on First Amendment grounds.[2] In a previous *Circuits* article, we examined that 2018 opinion, in which the Tyler Court of Appeals held that the statute was "an invalid content-based restriction and overbroad in the sense that it violates rights of too many third parties by restricting more speech than the Constitution permits."[3] And along the twisting road that culminated in the CCA's recent opinion in *Ex parte Jordan Bartlett Jones*, the 2019 Texas Legislature tweaked the law to address the Tyler court's concerns, by targeting only offenders who knowingly post "revenge porn" images with the intent to harm the person depicted. As the Tyler court's 2018 opinion had pointed out, the law (as earlier written) could apply to anyone reposting an image, even those who were unaware of the nonconsensual nature.[4]

In the May 26 opinion, the Court of Criminal Appeals held that while the law remained a content-based restriction, it passed constitutional muster since it was sufficiently narrowly tailored to a specific, compelling government interest—protecting sexual privacy. As the Court noted, "Disclosing visual material when the depicted person reasonably expected it would remain private is an intolerable invasion of privacy, especially when the visual material shows the depicted person's intimate parts or sexual conduct."[5] Rejecting arguments that the "revenge porn" law was vague to the point of possibly criminalizing protected behavior (like forwarding depictions of artwork or images relevant to public discourse), the Court observed that "there is no evidence that people who willingly participate in the creation of sexually explicit art commonly do so with any reasonable expectation of privacy, and the likelihood seems remote."[6]

---

1 *Ex parte Jones*, 2021 Tex. Crim. App. LEXIS 557 (Tex. Crim. App. May 26, 2021).
2 *Ex parte Jones*, _S.W.3d_, 2018 Tex. App. LEXIS 3439, 2018 WL 2228888 (Tex. App.—Tyler 2018).
3 *Id.* at *16.
4 *Id.*
5 *Ex parte Jones*, 2021 Tex. Crim. App. LEXIS 557, at *17.
6 *Id.* at *42.

Texas' "revenge porn" law not only makes the nonconsensual posting of intimate images a state jail felony punishable by up to two years in jail and a $10,000 fine, but it also allows victims to sue civilly for actual damages and mental anguish.

About the Author

John Browning is a former Justice on Texas' Fifth Court of Appeals, immediate past chair of the Computer and Technology Section of the State Bar, and a partner in the Plano office of Spencer Fane LLP.

Embattled Amazon Faces Another Courtroom Defeat

By John G. Browning

There is no question that Amazon has become an economic juggernaut. The e-commerce giant is adding 3,700 new sellers daily in 2021, and sales by third party vendors accounted for $386 billion, or 54% of Amazon's total net sales, in 2020. But in recent years, the company has been battling a wave of product liability suits nationwide, as consumers seek to hold Amazon strictly liable for allegedly defective products that it neither designed nor manufactured, but sold through its online marketplace. And while most of the cases have resulted in victories for Amazon, there are recent indications that the tide may be turning.

As I have chronicled in previous articles on this topic (see *Primed for Liability? Product Liability Exposure for E-Commerce Platforms* in March 2020 *Circuits*), Amazon has prevailed in a number of cases (including wins in the 6th and 9th Circuits), sometimes on grounds that Section 230 of the Communications Decency Act immunizes the platform against civil liability, and sometimes for not meeting a state's common law or statutory definition of being a "seller." However, a 3rd Circuit stalemate led to the Pennsylvania Supreme Court being asked to certify the question on whether Amazon was a "seller" (the case settled while on appeal), and the 5th Circuit similarly certified this question to the Supreme Court of Texas. In the latter case, *McMillan v. Amazon.com*,[1] oral arguments occurred earlier this year, and a ruling is expected by June.

And in California, things have not been going Amazon's way. In the 2020 case of *Bolger v. Amazon.com, LLC*,[2] California's Fourth District Court of Appeals held that (in a case involving a defective laptop battery that exploded) Amazon could be liable—even though it did not distribute, manufacture, or sell the product in question. The *Bolger* court found that Amazon was "a direct link in the chain of distribution, acting as a powerful intermediary between the third party seller and the consumer."[3] It reversed a summary judgment win for Amazon. The California Supreme Court denied review of this decision on November 18, 2020,[4] leaving the lower court's ruling intact.

---

1 983 F.3d 194 (5th Cir. Dec. 18, 2020).

2 53 Cal. App. 5th 431 (Aug. 13, 2020).

3 *Id.* at 438.

4 *Bolger v. Amazon*, 2020 Cal. LEXIS 7993 (Cal., Nov. 18, 2020).

In April, Amazon faced a case of déjà vu, only this time from California's Second Appellate District. In *Loomis v. Amazon.com LLC*,[5] Kisha Loomis brought personal injury claims for burns she suffered when a hoverboard she purchased on Amazon from a third party vendor, TurnUpUp, caught fire in her home in 2015. It was one of more than 380,000 hoverboards sold through Amazon that year. After hearing reports of problems with hoverboards, Amazon stopped selling them in December 2015. Within a few months, the Consumer Product Safety Commission issued a letter calling certain hoverboards a "substantial product hazard," and by July 2016, the CPSC announced recalls.[6]

Loomis lost at the trial court level. Amazon prevailed via summary judgment, arguing that it was outside the chain of distribution for product liability purposes. But on appeal, the justices at the Second Appellate District agreed with their counterparts in the *Bolger* case, reversing the summary judgment. The court pointed to California's judicially-created strict liability body of law, and particularly its public policy justifications. As Justice John Wiley wrote in a concurring opinion,[7]

> Once Amazon is convinced it will be holding the bag on these accidents, this motivation will prompt it to engineer effective ways to minimize these accident costs. Tort law will inspire Amazon to align its ingenuity with efficient customer safety. Customers will benefit. . . . Amazon is well-situated to take cost-effective measures to minimize the social costs of accidents.

Will Amazon's losing streak continue in Texas' *McMillan* case? Only time will tell. While Texas' products liability statute generally protects nonmanufacturing sellers from strict liability claims, there are exceptions. During oral argument, McMillan argued that Amazon is subject to liability based on three of those exceptions: that it knew of the defect; that it exercised control over the warning; and that the Chinese seller was beyond the jurisdiction of the court. The Court's eventual ruling could have a dramatic impact on e-commerce, not only in Texas, but nationally.

About the Author

John Browning is a former Justice on Texas' Fifth Court of Appeals, immediate past chair of the Computer and Technology Section of the State Bar, and a partner in the Plano office of Spencer Fane LLP.

---

5 63 Cal. App. 5th 466 (Apr. 26, 2021).

6 *Id.* at 474.

7 *Id.* at 488-489; 502 (Wiley, J., concurring).

Understanding the UPC

By Craig Ball

Where does the average person encounter binary data? Though we daily confront a deluge of digital information, it's all slickly packaged to spare us the bare binary bones of modern information technology. All, that is, save the humble Universal Product Code, the bar code symbology on every packaged product we purchase from a 70-inch TV to a box of Pop Tarts. Bar codes and their smarter Japanese cousins, QR Codes, are perhaps the most unvarnished example of binary encoding in our lives.

Barcodes have an ancient tie to e-discovery, as they were once used to Bates label hard copy documents, linking them to "objective coding" databases. A lawyer using barcoded documents was hot stuff back in the day.

Just a dozen numeric characters are encoded by the ninety-five stripes of a UPC-A barcode, but those digits are encoded so ingeniously as to make them error resistant and virtually tamperproof. The black and white stripes of a UPC are the ones and zeroes of binary encoding. Each number is encoded as seven bars and spaces ($12 \times 7 = 84$ bars and spaces) and an additional eleven bars and spaces denote start, middle and end of the UPC. The start and end markers are each encoded as *bar-space-bar* and the middle is always *space-bar-space-bar-space*. Numbers in a bar code are encoded by the width of the bar or space, from one to four units.

The bottle of Great Value purified water beside me sports the bar code at right.

Humans can read the numbers along the bottom, but the checkout scanner cannot; the scanner reads the bars. Before we delve into what the numbers signify in the transaction, let's probe *how* the barcode embodies the numbers. Here, I describe a bar code format called **UPC-A**. It is a *one-dimensional code* because it is read across. Other bar codes (*e.g.*, QR codes) are *two-dimensional codes* and store more information because they use a matrix that is read side-to-side and top-to-bottom.

The first two black bars on each end of the barcode signal the start and end of the sequence (*bar–space–bar*). They also serve to establish the baseline width of a single bar to serve as a touchstone for measurement. Bar codes must be scalable for different packaging, so the ability to change the size of the codes hinges on the ability to establish the scale of a single bar before reading the code.

#	Bar Code	#	Bar Code
0	3211	5	1231
1	2221	6	1114
2	2122	7	1312
3	1411	8	1213
4	1132	9	3112

Each of the ten decimal digits of the UPC are encoded using seven "bar width" units per the schema in the table at right.

To convey the decimal string 078742, the encoded sequence is **3211 1312 1213 1312 1132 2122** where each number in the encoding is the width of the bars or spaces. So, for the leading value "zero," the number is encoded as seven consecutive units divided into bars of varying widths: a bar three units wide, then (denoted by the change in color from white to black or vice-versa), a bar two units wide, then one then one. Do you see it? Once more, left-to-right, a white band, three units wide, a dark band two units wide, then a single white band and a single dark band (3-2-1-1 encoding the decimal value zero).

You could recast the encoding in ones and zeroes, where a black bar is a one and a white bar a zero. If you did, the first digit would be 0001101, the number seven would be 0111011 and so on; but there's no need for that, because the bands of light and dark are far easier to read with a beam of light than a string of printed characters.

Taking a closer look at the first six digits of my water bottle's UPC, I've superimposed the widths and corresponding decimal value for each group of seven units. The top is my idealized representation of the encoding, and the bottom is taken from a photograph of the label:

Now that you know how the bars encode the numbers, let's turn to what the twelve digits mean. The first six digits generally denote the product manufacturer. 078742 is Walmart. 038000 is assigned to Kellogg's. Apple is 885909 and Starbucks is 099555. The first digit can define the operation of the code. For example, when the first digit is a 5, it signifies a coupon and ties the coupon to the purchase required for its use. If the first digit is a 2, then the item is something sold by weight, like meats, fruit or vegetables, and the last six digits reflect the weight or price per pound. If the first digit is a 3, the item is a pharmaceutical.

Following the leftmost six-digit manufacturer code is the middle marker (1111, as *space-bar-space-bar-space*) followed by five digits identifying the product. Every size, color, and combo demands a unique identifier to obtain accurate pricing and an up-to-date inventory.

The last digit in the UPC serves as an error-correcting check digit to ensure the code has been read correctly. The check digit derives from a calculation performed on the other digits, such that if any digit is altered the check digit will not match the changed sequence. Forget about altering a UPC with a black marker: the change would not work out to the same check digit, so the scanner will reject it.

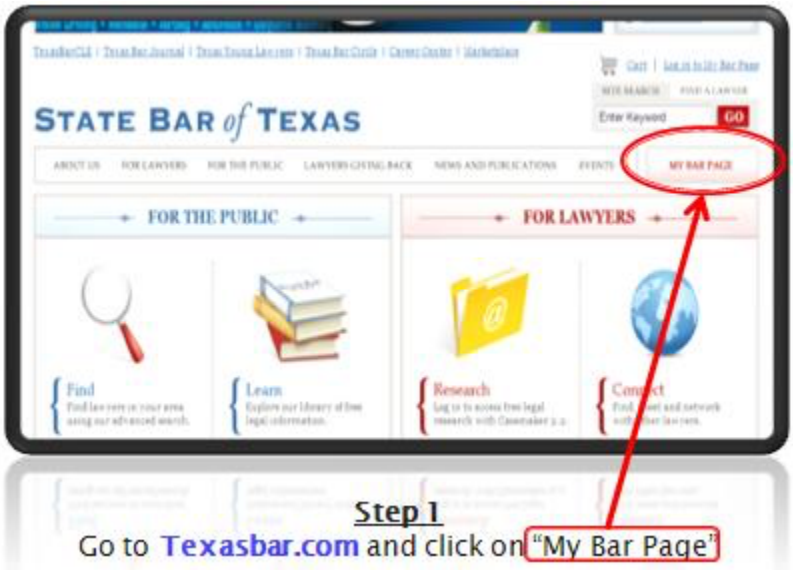
In case you're wondering, the first product to be scanned at a checkout counter using a bar code was a fifty-stick pack of Juicy Fruit gum in Troy, Ohio on June 26, 1974. It rang up for sixty-seven cents. Today, 45 sticks will set you back $2.48 (UPC 22000109989).

About the Author

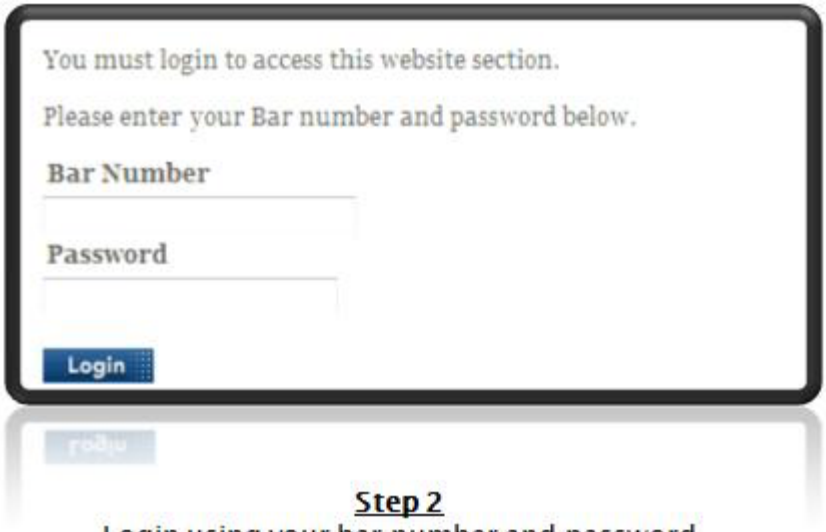
Craig Ball teaches Electronic Evidence at the University of Texas and Tulane University Schools of Law. He limits his practice to service as a Special Master in eDiscovery and Computer Forensics.

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:
Shawn Tuma – Plano – Chair
Elizabeth Rogers – Austin – Chair-Elect
Pierre Grosdidier – Houston – Treasurer
Reginal Hirsch – Houston – Secretary
John Browning – Dallas – Past Chair

Circuits Editors:
Sanjeev Kumar – Austin
Kristen Knauf – Dallas

Webmasters:
Ron Chichester – Houston
Rick Robertson – Dallas

Appointed Judicial Members:
Judge Xavier Rodriguez – San Antonio
Hon. Roy Ferguson – Alpine

Term Expiring 2022:
Lavonne Burke Hopkins – Houston
Gwendolyn Seale – Austin
Alex Shahrestani – Austin
Michelle Mellon-Werch – Austin

Term Expiring 2021:
Chris Downs – Plano
Seth Jaffe – Houston
Judge Emily Miskel – Dallas
William Smith – Austin

Chairs of the Computer & Technology Section

2019-2020: John Browning
2018-2019: Sammy Ford IV
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