COMPUTER AND TECHNOLOGY SECTION

Circuits

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

Table of Contents

Featured Articles

Short Circuits

Table of Contents

Feature Articles:-

Short Circuits:-

Message from the Chair

By Shawn E. Tuma

Happy New Year and welcome to another issue of *Circuits*! The Computer & Technology Section had an outstanding year in 2020 and we are working very hard to make 2021 even better. We thank you for being a member and hope that you will help us spread the word by urging your colleagues to join as well.

We closed out last year with our 4th annual *With Technology and Justice for All* conference, a one-day CLE course. The conference theme was *Vaccinating Your Technology Tools for Practice in a Pandemic* and, though it was held virtually for the first time, the presentations were as relevant and outstanding as ever. Thank you to everyone who participated in and attended the conference; we are already looking forward to next year's!

The importance of the intersection of law and technology has never been more vital than it is right now. For example, in cybersecurity, the news in December of the successful cyber-attack on FireEye, one of the world's preeminent cybersecurity companies, proved that if it could happen to them, it truly can and likely will happen to any organization. This quickly led to the discovery of how the attack occurred: the highly sophisticated SolarWinds compromise which involved a stealthy attack on SolarWinds' Orion network management tool that was used by information technology service providers and companies themselves throughout the world, demonstrating the importance and impact of third-party supply chain cyber risk.

As the COVID-19 pandemic continues, we are continuing to see privacy issues arise with the use of technology in contact tracing and tele-medicine. The pandemic is also leading to the overall transformation of how we live and work by leveraging technology to work from remote environments without being tethered to an office. While most of us think of this in terms of working from home, some attorneys are either moving their homes to, or staying for long periods of time in, remote new locations in different jurisdictions, thereby raising potential ethical issues regarding the unauthorized practice of law.

As we moved into January, we began seeing increased public discussion about the impact of technology on basic issues of humanity as "big tech" continued taking a more active role in controlling the content of information being communicated through its platforms and infrastructure, raising questions about the intersection of technology, freedom of expression, and censorship as our lives become more and more intertwined with the digital realm.

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 Working Group
- 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

Our State Bar Annual Meeting is coming up in June in Fort Worth. Please try to join us at our annual membership meeting as we vote on a new slate of Officers and Council Members. The Annual Meeting will include outstanding programming featuring many Section Members on a broad range of cutting-edge law and technology subjects, including the popular Adaptable Lawyer Track.

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.

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

COMPUTER AND TECHNOLOGY SECTION

Letter from the Editor

By Sanjeev Kumar

Welcome to the second issue of *Circuits* eJournal for the 2020-21 bar year! As I write this letter, Texas is going through a historic freeze that has left millions of our citizens without power, heat and water. The roads have been impossible for even short trips and working from home, if you are fortunate enough to have power and Internet connection, has become a necessity for most of us.

Perhaps more fortunately this year than ever before, the Computer and Technology Section has a lot of tools available to help us lawyers remain productive remotely in our practice. Or, if you are looking to take a break from remote work, one of our ex-chairs, Joseph Jacobson, has informed me that National Cryptologic Museum is open for virtual tours. If you feel so inclined, please check it out at https://www.nsa.gov/about/cryptologic-heritage/museum/.

The need to work remotely as a result of the COVID-19 pandemic and recent inclement weather has resulted in increased use of electronic collaboration tools. Remote work has also increased the threats to the safety of our data and operations. So, we felt it would be timely to provide some helpful tips for safely working from home. As a result, we start our Feature Articles with a contribution from Section Chair Shawn Tuma, who discusses five things we practitioners should be doing while working from home to be cyber secure in an article originally published in the Texas Bar Journal and reprinted with permission.

Next, our Council Member, Judge Emily Miskel, provides guidance to practitioners on how to best compel direct access to electronic data in her Feature Article on eDiscovery. She discusses a couple of Texas cases on the subject and provides guidance on prerequisites for success in compelling direct access.

News about bitcoins, blockchains and artificial intelligence have proliferated the news in the recent past and have also raised numerous novel questions of law. Some states have even changed their laws to allow for these emerging technologies. Our past Section Chair and current council member, Ron Chichester, provides a crash course in blockchain technology and smart contracts in our next Feature Article on how to incorporate an entirely digital corporation.

The virtual trials resulting from the COVID-19 pandemic have raised numerous novel issues with court procedures and trial records. In our next Feature Article, Judge Miskel discusses the interplay of these issues with existing rules dealing with trial records and evidence.

Last but not least our past Section Chair, Judge John Browning, discusses the morphing laws related to bystander recovery as a result of emerging new technologies and the associated effects on our day-to-day activities.

We start our Short Circuits section with a supplementary article by Judge Miskel to her feature article, in which she discusses direct access to electronic data by means of the type of electronic data at issue and provides some example cases.

Next, our past-chair, Judge Browning, discusses the conflicts and issues caused by emerging technologies on legal rules such as hearsay.

We continue our Short Circuits section with two articles from our former Section Chair and my predecessor as the Editor of *Circuits* eJournal, Pierre Grosdidier. In his first Short Circuit, he discusses the interplay of legislation with First Amendment rights, specifically as related to cyberstalking and cyberbullying. Next, he discusses the issues caused by the combination of technology and involvement of private parties as related to Fourth Amendment rights.

The next Short Circuit is penned by our past Section Chair and current council member, Ron Chichester. He discusses the complexities of applying laws meant for people to activities that are enabled by computer technology and automated data analysis tools.

Short Circuits continues with two additional offerings from our past-chair Judge Browning. In the first article, Judge Browning discusses the duties and responsibilities of social media platforms, such as Facebook, when users of the platform post notice of their intent to engage in possible nefarious activity, even murder, when it actually materializes. In his next offering, Judge Browning discusses the unsettled and emerging landscape of ecommerce platform providers' possible liability in product liability cases.

The next Short Circuit article is penned by our Chair-Elect, Elizabeth Rogers, who discusses the current status of specializing in privacy law in Texas. This is a follow-up to her publication in the last issue, which assisted the legal community in better serving our business clients by adopting certain processes to avoid unintentional violation of regulatory regimes.

I frequently come across clients in my business law practice whose trademark has been infringed on or is being used to impersonate them on a fake website or similar domain name.

Guest writer Richard Beem discusses the many ways unscrupulous characters misuse other's success and provides a quick guide on how best to take down fake websites in the first article in our Circuit Boards Section.

Considering the charged political theater we have witnessed during this election cycle, without any political leanings, we end this issue of *Circuits* with an article about the lawyer's oath by our judicial council member, Judge Xavier Rodriguez, which should make us all think and evaluate what we each should strive to uphold.

Many thanks to all the contributors to this new issue. A big thank you also to Kirsten Kumar for her review of and assistance with this issue's articles. We hope that you enjoy this new edition of *Circuits* eJournal and as always, we welcome any comments that you may have. Please send them to our section administrator at admin@sbot.org.

Kind Regards,
Sanjeev Kumar, Co-Editor

FEATURE ARTICLES:-

Working From Home During COVID-19

Five things you should be doing—but probably are not—to be more cyber secure.

By Shawn Tuma

March 2020 will go down in history as marking a quantum leap in the way we lawyers do business from a primary office-based environment to an almost exclusively work-from-home environment. A transition that, under normal circumstances would have taken many years, took place within hours or, maybe, a few days, as shutdown orders forced people to stay out of their offices and to work from home. There was no time to plan ahead for this transition and most had to adapt on the fly and do the best we could. As much as this pandemic impacted the way we live our lives, it impacted the cybersecurity of our practices as well as our clients' businesses.

The Pandemic Marked a Quantum Leap in our Lives, Work, and for Cyberrisk

Cyberrisk is not a new concept. The words "cybersecurity," "data privacy," and "data breach" have been an increasing part of our vocabulary since the headline data breaches of 2013. For lawyers in particular, the trend is the same. Hackers consistently target law firms because they see them as a one-stop-shop treasure trove of valuable information. As a result, several prominent law firms have made the news for their cybersecurity events, well over 100 law firms have publicly reported data breaches, and at least one prominent law firm, Mossack Fonseca, closed its doors following a data breach that revealed the Panama Papers.

In the world of cybersecurity, the odds are stacked against you from the beginning, as your security must get it right 100% of the time while a threat actor only needs one lucky shot for an attack to succeed. Those odds get worse as your network environment increases and becomes less controlled because the larger your environment is, the more targets threat actors have to attack.

Prior to COVID-19, it was difficult enough to protect computer networks and the information contained thereon when the "network" was primarily contained within the controlled environment of office space in professional office buildings in one or more locations (for those law firms that had multiple offices). While there were those power users who would take their laptops and work remotely while out of the office, they were still the exception, not the norm, as most firm employees were still working in the office.

When COVID-19 sent everyone working from home all of the time, the threat landscape increased exponentially. The only way most firms could adapt was to find ways to provide employees with access to their network from wherever they were located. With all employees being out of the controlled office environments, that network literally expanded to include every location where every employee was located. To provide for communications that were usually done face-to-face, many turned to third-party services that had not been vetted and for which there was no training and no uniform setup process to ensure they were used in as secure of a manner as possible. This led to new trends such as "Zoom-bombing."[1]

FBI's COVID-19 Remote Work Cybersecurity Prevention Tips Are Required Reading for All

In April 2020, the FBI reported a spike in cybercrime activity since the beginning of the pandemic, with the Internet Crime Complaint Center receiving about 3,000-4,000 complaints a day as compared to 1,000 complaints a day shortly before the pandemic.[2] The FBI issued a public service announcement, or PSA,[3] addressing this increase in threats. The PSA included an extensive explanation of each of the common threats as well as actionable tips for preventing the most common threats.

Everyone should carefully read the FBI's tips in the PSA, as they are easy to understand and are just as applicable for improving cybersecurity when life returns to normal as they are during a pandemic. There are too many tips to include in this article, but the PSA is linked in the endnotes.

Top Five Things We See Organizations Not Doing—That They Should Be Doing—That Lead to Cyber Incidents and Data Breaches

In my practice, I advise and lead organizations through the process of investigating and responding to cyber incidents and data breaches. In this role, our team comes in after an event has occurred and, among other things, works with technical cybersecurity experts to assist in

---

1 For tips to prevent Zoom-bombing, see my article *Understanding the Cyber and Privacy Risks of Zoom and Tips for Using it More Securely* (Apr. 3, 2020), https://www.spencerfane.com/publication/understanding-the-cyber-and-privacy-risks-of-zoom-and-tips-for-using-it-more-safely/.

2 Maggie Miller, *FBI sees spike in cyber crime reports during coronavirus pandemic,* The Hill (Apr. 16, 2020), https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic.

3 FBI PSA: Cyber Actors Take Advantage of Covid-19 Pandemic to Exploit Increased Use of Virtual Environments (Apr. 1, 2020), https://www.ic3.gov/media/2020/200401.aspx.

investigating to learn how and why it occurred, as well as how it could have been prevented. Though I am still just a lawyer, I have learned a lot over the years.

When asked what organizations can do to help improve their cyberrisk posture, the safest answer is always "everything!" Reasonable cybersecurity experts could offer enough tips and advice to fill volumes and, while many would be similar, many would not be and the order of priority would vary significantly. I have my own "Good Cyber Hygiene Checklist"[4] but, in the world of cybersecurity, much like in the legal profession, the answer to the question of "what is best?" is often "it depends." Unfortunately, there is so much information and misinformation out there that many organizations end up not taking any action because they cannot determine how to prioritize or where to begin.

Without an understanding of the particular organization or the unique risks it faces, it is impossible to know what is best or most important. What we do know is what we are seeing organizations not doing—that they should be doing—that most frequently leads to cyber incidents and data breaches. The following five recommendations address what we see exploited most often that are not always on the top of organizations' priorities.

1. Backups, Backups, Backups!

There is another pandemic going around called ransomware and the odds of it infecting your organization are high. For years we heard, "We do not worry about cybersecurity because our data is not that valuable." The threat actors learned that regardless of how valuable data was to others, data was valuable to the organization itself and, if they could encrypt the organization's data and make it unavailable, the organization would pay a ransom to regain access to it. Quickly realizing that when an organization had viable backups of their data they would not pay, they adapted their tactics and now, upon first gaining access to the network, locate the backups of the data and either delete or infect the backups, then launch the primary ransomware attack. Organizations must have a backup strategy that accounts for this threat such as the "3-2-1 backup rule," which is:

3) have a least three copies of your data;
2) store the copies on two different media; and
1) keep at least one backup copy disconnected and offsite.

Simply having backups is not enough—you must use a strategy such as this and recognize that the last copy, the one kept offsite, may be all you have left to carry on your operations.

---

[4] Good Cyber Hygiene Checklist, https://www.spencerfane.com/wp-content/uploads/2019/02/Cyber-Hygiene-Checklist.pdf.

2. Multifactor Authentication, or MFA.

Every login for something important must require MFA, which is using two steps to login instead of just one. For example, MFA would require a password plus clicking an app on your phone before you could successfully login. If you are using Microsoft Office 365, Google, or another form of cloud-accessible email, you should be absolutely certain you have implemented MFA.

3. Phishing Training and Exercises.

Phishing emails continue to account for the vast majority of attacks on organizations and continue to be effective at delivering malware, viruses, harvesting login credentials, and triggering other fraud schemes such as the business email compromise. One of the most effective ways to combat the threat of phishing emails is by training members of the workforce to recognize phishing emails and then having regular exercises to test them by sending fake phishing emails to see who is clicking on the links or otherwise falling for the phishing email.

4. Remote Desktop/Virtual Network Computing.

Do not permit remote desktop protocol or virtual network computing unless necessary. If you do permit it, require that it only be used with a reputable encrypted virtual private network that requires MFA to access.

5. Disk Encryption.

Every device that can reasonably be transported from one location to another by an individual should have full disk encryption enabled. Hackers do love to hack but thieves also love to steal and people have a bad habit of leaving devices in the Uber or sitting at the airport. Having encryption enabled could mean the difference between just replacing a lost piece of hardware versus exposing sensitive information on that device and having to notify the world of a data breach.

This article was originally published in the Texas Bar Journal and has been reprinted with permission.

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.

eDiscovery – How to Compel Direct Access to Electronic Data

By Judge Emily Miskel

In the traditional discovery process, a party sends production requests to her opponent, who must search his own files to produce responsive documents. A requesting party typically cannot demand to go to her opponent's place of business and search through his file cabinets herself. That would be considered "direct access" to the opposing party's information.

In eDiscovery, it is common for parties to seek direct access to their opponents' electronically stored information ("ESI"). Parties doubt that their opponents are truly producing all responsive information, whether they are intentionally withholding information or whether they lack the technological competence to thoroughly search and produce electronic information. Parties commonly pursue direct access to their opponents' ESI through methods such as:

- Requesting a login and password to download electronic or social media information,
- Requesting to have hard drives or cell phones forensically imaged, or
- Requesting a party to turn over an entire digital archive, so that the requester can peruse it and determine what is responsive.

While the court may shift the cost of the forensic examination to the requesting party, the burdens of direct access are not solely financial. "[S]ignificant harm can result from granting direct access . . . when direct access is not warranted; this harm arises from the risk of revealing private conversations, trade secrets, and privileged or otherwise confidential communications. This harm is not remedied by requiring the party seeking discovery to pay for the intrusion."[1]

In 2009 and again in 2018, the Texas Supreme Court reiterated that direct access to electronically stored information is intrusive and should be discouraged. Without actual evidence, not mere suspicion, that a party is committing discovery abuse or failing in their discovery obligations, the opposing party should not have direct access to ESI.

A. *In re Weekley Homes* (Tex. 2009)

A key opinion by the Texas Supreme Court governing electronic discovery was published in 2009.[2] In a lawsuit over a subdivision development, the plaintiff HFG sought documents from the homebuilder Weekley Homes, including emails from employees relating to the

---

[1] *In re Methodist Primary Care Grp.*, 553 S.W.3d 709, 720 (Tex. App.—Houston [14th Dist.] 2018.

[2] *In re Weekley Homes, L.P.*, 295 S.W.3d 309 (Tex. 2009).

development. Weekley Homes produced just 31 responsive emails, including only one email discussing a critical engineering analysis.[3] The plaintiff HFG did not believe that these were the only emails that existed and moved to allow forensic experts to image four employee hard drives to determine whether deleted emails were on the devices.[4] The trial court ordered that forensic experts would image the hard drives and search for deleted emails relating to a list of key words. Once any responsive documents were identified, Weekley Homes would have the right to review its data, designate which documents were privileged or not discoverable, and produce responsive documents to HFG.[5]

The Texas Supreme Court reviewed federal rules and federal case law approvingly, noting that "ordering examination of a party's electronic storage device is particularly intrusive and should be generally discouraged, just as permitting open access to a party's file cabinets for general perusal would be."[6]

The Court described several reasons why it was an abuse of discretion for the trial court to compel direct access:

- Failed to prove that the defendant defaulted in its discovery obligations,
- Did not prove that the benefit of the forensic examination would outweigh the burden of the invasive method,
- Relied primarily on discrepancies and inconsistencies in the production and concern about the limited number of emails,
- Insufficient evidence to show that a search of the employee hard drives would likely reveal deleted emails, other than conclusory statements that deleted emails must exist, and
- No evidence about the particularities of the company's electronic information storage, whether it would allow retrieval of deleted emails, and what the retrieval would entail.

The Texas Supreme Court noted that "while direct access to a party's electronic storage device might be justified in some circumstances, the rules are not meant to create a routine right of direct access."[7]

---

3 *Id.* at 312.
4 *Id.* at 313.
5 *Id.*
6 *Id.* at 317.
7 *Id.*

B. *In re Shipman* (Tex. 2018)

In 2018, the Texas Supreme Court again encountered a dispute about the standard for direct access to a party's electronically stored information.[8] In this case, the requesting party had concerns about the responding party's technical ability to search and produce the information.

Marion Shipman and Jamie Shelton had discovery disputes in connection with a lawsuit by a bank. In Shipman's deposition, he testified that he produced all the documents in his possession, but he was unable to retrieve some records from an old computer that crashed.[9] Several days later, Shipman produced additional documents, reporting that his son helped him discover files from the old computer in a backup folder. He also submitted an affidavit that he had destroyed files more than 7 years old, that he had diligently searched his physical and electronic files, and that he had produced all responsive documents.[10]

The trial court ordered Shipman to produce his computer and all media (thumb drives, hard drives, CDs, etc.) that he had used since 2000. A forensic examiner would provide a list of all file names to Shipman, who could object before producing anything. Shipman objected that the evidence did not show that he had defaulted on his discovery obligations, that his production was inadequate, or that a forensic search could recover responsive materials.[11] Further the trial court's order was overbroad, in that it covered all data for the past 17 years and granted more relief than was requested.

The Texas Supreme Court stated that, before "granting access to electronic devices, the requesting party must show that the responding party has somehow defaulted in its obligation to search records and produce the requested data."[12] The trial court should not rely on "mere skepticism or bare allegations that the responding party has failed to comply with" discovery duties.[13]

Shelton relied on the following facts to show discovery abuse:

- Shipman's deposition testimony claimed no documents existed, but days later, he found and produced documents,

---

8 *In re Shipman*, 540 S.W.3d 562 (Tex. 2018) (per curiam).
9 *Id.* at 564.
10 *Id.*
11 *Id.* at 565.
12 *Id.* at 567.
13 *Id.*

- Shipman lacked the expertise to thoroughly and diligently search electronic storage media, and
- Shipman gave equivocal answers about what documents he thought he had.

The Court found that these complaints amounted to mere skepticism that responsive documents remain on the computer, and it was insufficient evidence to find that he defaulted on his discovery obligations.[14] Nor did Shelton elicit any evidence about Shipman's computer skills or the specific steps he took to search his computer. The Court noted, "We do not suggest that a requesting party can never establish a discovery-obligation default . . . by offering evidence of a producing party's technical ineptitude . . . But the burden imposed by *Weekley* is high—forensic examination of electronic devices is 'particularly intrusive and should be generally discouraged.'"[15]

C. How to Compel Direct Access

First, the requesting party must make a specific request for electronic data under Tex. R. Civ. P. 196.4. For example, compelling a party to turn over computer and network server hard drives without requiring the requestor to identify specific discovery requests does not follow the requirements of Rule 196.4 and *Weekley Homes*, and is an abuse of discretion.[16]

Second, the requesting party must present evidence showing that the responding party defaulted in her discovery obligations. Mere skepticism and bare allegations are not evidence, and neither are conclusory statements that evidence must exist.

Third, the requesting party must establish that data retrieval is feasible.[17] The requesting party must show, with evidence, that the intrusive direct access would likely reveal the information, or that it would be reasonably capable of recovery.[18]

Fourth, the requesting party must show that the benefits of the discovery outweigh the burden imposed on the responding party.[19] "The least intrusive means of providing relevant, responsive information should be employed."[20]

---

[14] *Id.* at 569.

[15] *Id.*

[16] *In re Pinnacle Eng'g, Inc.*, 405 S.W.3d 835, 842 (Tex.App.—Houston [1st Dist.] 2013).

[17] *See In re Stern*, 321 S.W.3d 828, 846 (Tex.App.—Houston [1st Dist.] 2010).

[18] *See In re Weekley Homes*, 295 S.W.3d at 319-20; *In re Pinnacle Eng'g, Inc.*, 405 S.W.3d at 844.

[19] *See In re Weekley Homes*, 295 S.W.3d at 322; *In re Clark*, 345 S.W.3d 209, 212 (Tex.App.—Beaumont 2011).

Fifth, the direct access protocol must reflect evidence that a qualified expert will conduct the investigation and there are specific limitations and guidelines as to how the expert would conduct the searches.[21] A court may not give the expert "carte blanche authorization to sort through the responding party's electronic storage device."[22] The protocol should also provide guidelines as to how the expert would protect confidential and privileged documents.[23] "Absent some evidence that the expert is familiar with the particularities of the storage device to be searched, that the expert is qualified to search those devices, and that the proposed methodology for searching the devices is reasonably likely to yield the information sought, an order allowing direct access is not proper."[24]

Finally, "courts have been more likely to order direct access to a responding party's electronic storage devices when there is some direct relationship between the electronic storage device and the claim itself."[25] For example, where employees were alleged to have used company computers to forward trade secrets to their personal email accounts, it was justified to forensically examine the employees' personal computers.[26]

D. Conclusion

The traditional rules of discovery apply to electronic and social media discovery. However, detailed evidence is required to obtain direct access to an opponent's files. Attorneys should not be intimidated from seeking electronic discovery, but should review Texas Supreme Court case law in detail before attempting to compel electronic production.

About the Author

Judge Emily Miskel of the 470th district court of Collin County, Texas, was appointed by Gov. Greg Abbott in 2015. She is board certified in family law by the Texas Board of Legal Specialization. Judge Miskel has an engineering degree from Stanford University, and she received her law degree from Harvard Law School. Before she was judge of the 470th district court, she practiced family law in Plano, Texas.

---

[20] *In re VERP Inv., LLC*, 457 S.W.3d 255, 261 (Tex. App.—Dallas 2015).

[21] *In re Pinnacle Eng'g*, 405 S.W.3d at 845; *see also In re Clark*, 345 S.W.3d at 213.

[22] *In re Pinnacle Eng'g*, 405 S.W.3d at 845.

[23] *Id.* at 846.

[24] *In re VERP Inv.*, 457 S.W.3d at 263.

[25] *In re Weekley Homes*, 295 S.W.3d at 319.

[26] *Id.* (referencing *Ameriwood Indus., Inc. v. Liberman*, No. 4:06CV524-DJS, 2006 U.S. Dist. LEXIS 93380, at *5 (E.D. Mo. Dec. 27, 2006)).

How do You Incorporate an Entirely Digital Corporation?

By Ronald Chichester

1. Abstract

This paper describes what attorneys need to know about incorporating companies that rely heavily – if not exclusively – on blockchains. Because technology is central to this topic, references will be provided for a brief introduction to: cryptocurrencies, blockchains (which is the underlying technology to cryptocurrencies), smart contracts, and distributed autonomous organizations. Finally, this paper will discuss the peculiar requirements for incorporating a blockchain-based company.

2. What is a Cryptocurrency?

Most people's introduction to blockchains comes from their experiences with cryptocurrencies. According to Forbes, a "[c]ryptocurrency is decentralized digital money, based on blockchain technology."[1] Examples of cryptocurrencies include Bitcoin[2] and Ethereum.[3] Ethereum has the added benefit of executing code that controls digital value.[4] Essentially, cryptocurrencies enact a different trust paradigm, wherein middle*men* (banks and governments) are replaced by middle*things* (computers and networks). Cryptocurrencies rely on three major elements: peer-to-peer networking,[5] encryption,[6] and game theory.[7] As with most national currencies, most cryptocurrencies are fiat, in that they are not backed by some finite commodity, such as gold. Cryptocurrencies are essential for monetary transactions involving blockchain-based companies. Once companies and individuals have accounts (addresses) on a particular cryptocurrency, that company or individual may conduct transactions with any other individual

---

1 Kate Ashford and John Schmidt, *What is Cryptocurrency?*, Forbes Advisor (Dec. 18, 2020) https://www.forbes.com/advisor/investing/what-is-cryptocurrency/.

2 Bitcoin, https://bitcoin.org/en/ ("Bitcoin is an innovative payment network and a new kind of money.") (last visited Feb. 6, 2021)..

3 Ethereum, https://ethereum.org/en/ ("Ethereum is the community-run technology powering the cryptocurrency, ether (ETH), and thousands of decentralized applications.") (last visited Feb. 6, 2021).

4 *See id.*

5 *See, e.g.,* Peer-to-peer, WIKIPEDIA, https://en.wikipedia.org/wiki/Peer-to-peer (last visited Feb. 6, 2021).

6 *See, e.g.,* Encryption, WIKIPEDIA, https://en.wikipedia.org/wiki/Encryption (last visited Feb. 6, 2021).

7 *See, e.g.,* Game theory, WIKIPEDIA, https://en.wikipedia.org/wiki/Game_theory (last visited Feb. 6, 2021).

or company that has access to the same cryptocurrency. There are also exchanges for cryptocurrencies, such as Binance.[8]

3. What is a Blockchain?

The underlying technology used to implement a cryptocurrency is called a *blockchain*. A blockchain is a computerized ledger that is suitable for use within an organization, or within multiple organizations and individuals. Note, in many jurisdictions, blockchains are often referred to (generically) as *distributed ledgers*.

Blockchains have two or more physical components: at least one *node* and a way to get information to/from the nodes. Each node in the blockchain is running identical software precisely so it can process transactions like every other node. The software can be open source or it can be proprietary, but it must be identical to every node on the blockchain.[9] The software running on the node validates (or does not validate) the transactions. If there is more than one node, they are typically connected to each other by a peer-to-peer network. Users place their transactions on the peer-to-peer network, and the nodes race to validate it. If validated, the transaction is encrypted and the encrypted record is inserted into a block. Then the block is cryptographically *hashed*[10] and that hash value can be shared with the other nodes to ensure that all of the nodes agree. Typically, once at least half the nodes agree on the validity of the transaction, then the transaction is considered validated. Each block is then hashed with all previous blocks to form a chain of blocks, hence the name blockchain. Generally, if a node's hash does not comport with the other nodes, then that node replicates the blocks from the other nodes to bring itself into compliance. There is an incentive for the nodes to comport with each other. If a node is not compliant, it cannot be trusted to execute further transactions, rendering that node useless to the blockchain and the owner of the node precluded from remuneration for hosting that node.

While there is no standard architecture for blockchains, in general, most are considered either *public* or *private*. Private blockchains are controlled by a single entity and are generally used to facilitate transactions between a small group of trusted entities. Public blockchains, however, are available to the public for transactions between any set of companies or individuals that

---

8 Binance, https://www.binance.com/en (last visited Feb. 6, 2021).

9 For example, Bitcoin node software is open source, and is available at: https://bitcoin.org/en/full-node.

10 *See, e.g.,* Cryptographic hash function, WIKIPEDIA, https://en.wikipedia.org/wiki/Cryptographic_hash_function (last visited Feb. 6, 2021).

don't need to trust each other. Bitcoin is an example of a cryptocurrency that is on a public blockchain.

The design of the blockchain is vital to the purpose of the resulting transactions. While the basic design of blockchains *can* be robust and secure, the design decisions enacted can affect *how* robust and secure the resulting blockchain will be. The linchpin for blockchain design is the number (and ownership) of the nodes. The greater the number of nodes (and owners), the more robust the blockchain because the more difficult it is to validate an improper transaction. Unfortunately, this design makes it difficult to update the software for the nodes, as is intended. However, updates and/or hostile takeovers of a blockchain are possible, and that process is called a *fork*.[11] How easy (or difficult) it is to fork a particular blockchain design is an important risk factor for investors.

A truly detailed introduction to blockchains is outside the scope of this article. Fortunately, there are many good introductions to blockchain on the Web and YouTube, and I commend your attention to those resources.[12] For a detailed explanation of the trust paradigm (and legal implications thereof) made possible by blockchains, see the seminal book on blockchains and resulting trust paradigms by Kevin Werbach.[13]

4. What is a Smart Contract?

"A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible."[14] The code can run on a non-proprietary cryptocurrency blockchain, such as Ethereum, or on a private blockchain. When a software application is implemented on a distributed blockchain, that application is called a "dapp"; a smart contract is an example of a dapp.[15] Incidentally, private blockchains are easy to

---

[11] *See, e.g.,* Coin Idol, *Definition of a Cryptocurrency Fork; Why Are They Necessary?*, Coin Idol.com (Feb. 9, 2020), https://coinidol.com/definition-cryptocurrency-fork/.

[12] *See, e.g.,* How does a blockchain work - Simply Explained, YOUTUBE (Nov. 13, 2017), https://www.youtube.com/watch?v=SSo_EIwHSd4.

[13] KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST (Massachusetts Institute of Technology 2018).

[14] Jake Frankenfield, *What Is a Smart Contract?*, Investopedia (Oct. 8, 2019) https://www.investopedia.com/terms/s/smart-contracts.asp.

[15] *See, e.g.,* Introduction to Dapps, Ethereum Developer Documentation (Jan. 12, 2021) https://ethereum.org/en/developers/docs/dapps/.

set up. Much of the software is open source[16] and readily available. In fact, you can set up your own Ethereum blockchain for development purposes using software such as Truffle and Ganache.[17] This means that the cost of entry for a cryptocurrency is very low, which accounts for their proliferation.

When two companies consummate a smart contract, the software code that describes the terms of the contract are placed (instantiated) onto, for example, the Ethereum blockchain. The goal of a smart contract is to automate the compliance of the terms as much as possible, and not to rely on human interaction or intervention. To that end, reliance is placed on electronic devices that are often part of the "Internet of Things" ("IoT"), which are capable of conducting transactions on the same blockchain as the smart contract. For example, an automaker could contract for 500,000 spark plugs from a vendor through a smart contract in Ethereum. The code for the smart contract may expect a signal from an IoT device when an individual spark plug leaves the factory and trigger a micro-payment to the spark plug manufacturer upon that event with Ether cryptocurrency. Final payment could be made upon detection (by another IoT device) of the delivered spark plug at the automaker's factory. All of the terms of the contract are reflected in the code. All remedies for problems may also be reflected in the code, which thus precludes parole evidence and (most) potential lawsuits. Contractual language can thus be commoditized and thereby reducible to rigid computer code that is known by (and testable by) both parties using an agreed-upon set of code. Workflows that define the process of the contract can be defined in a domain-specific language, such as *Legalese.*[18] Software frameworks, such as Brownie,[19] exist that simplify the process of drafting and implementing a smart contract.

---

[16] For more information about open source software, *see* https://opensource.org/.

[17] CodeOoze, *How to install Truffle and Ganache in Ubuntu 18.04*, CodeOoze.com (Feb. 17, 2019) https://www.codeooze.com/blockchain/ethereum-dev-environment-2019/. Ganache is a quick and easy way to run a personal blockchain for developing and deploying smart contracts. Truffle is used to manage smart contract projects, testing, compiling and migration. *Id.*

[18] Legalese, https://legalese.com/ (last visited Feb. 6, 2021).

[19] Brownie is a Python-based development and testing framework for smart contracts targeting the Ethereum Virtual Machine. *See* Github, https://github.com/iamdefinitelyahuman/brownie-v2. *See also*, Saurav Verma, *Learn the Basics of Brownie*, Better Programming (Jan. 31, 2020), https://medium.com/better-programming/part-1-brownie-smart-contracts-framework-for-ethereum-basics-5efc80205413.

5. What is a Distributed Autonomous Organization ("DAO")?

"With smart contracts, a blockchain network gains the power of automated decision-making and execution."[20] "[T]hat capability can be used to create a new algorithmic organizational form: the distributed autonomous organization, or DAO."[21] Under the "nexus of contracts theory" of corporations, a company is nothing more than a set of contracts.[22] Similarly, a set of smart contracts are said to form a DAO.[23] Essentially, "[t]he standard corporate arrangements of equity, debt, and corporate governance can be encoded in a series of smart contracts based on cryptocurrencies."[24]

Examples of DAOs include DAOstack,[25] Jelurdia,[26] MakerDAO,[27] and Moloch DAO.[28] While at the moment, many DAOs are themselves devoted to the automation of DAO-creation, the Moloch DAO is devoted to funding startups that are themselves DAOs. As one might expect, this automation craze has prompted engineers to develop a framework for automating the

---

[20] Werbach, *supra* note 14, at 110.

[21] *Id.*

[22] *See, e.g.,* Ronald F. White, *Nexus of Contracts Theory*, College of Mount St. Joseph, http://faculty.msj.edu/whiter/nexusofcontracts.htm (this article takes an economist's view of the theory). *See also,* Soumik Chakraborty, *Corporation As Nexus of Contracts: A Critque*, Academike (Dec. 17, 2014), https://www.lawctopus.com/academike/corporation-nexus-contracts-critique/ ("*The nexus of contracts theory is an idea put forth by a number of economists and legal commentators which asserts that corporations are nothing more than a collection of contracts between different parties – primarily shareholders, directors, employees, suppliers, and customers"); William W. Bratton Jr., Nexus of Contracts Corporation: A Critical Appraisal, 74 Cornell L. Rev. 407 (1989), http://scholarship.law.cornell.edu/clr/vol74/iss3/1*.

[23] *See, e.g., Distributed autonomous organization*, Platform Value Now (Mar. 2, 2017), https://platformvaluenow.org/signals/distributed-autonomous-organization/; Werbach, *supra* note 14, at 110.

[24] Werbach, *supra* note 14, at 110.

[25] DAOstack, https://daostack.io/ ("DAOstack is an open source project advancing the technology and adoption of decentralized governance.") (last visited Feb. 6, 2021).

[26] Jelurida, https://www.jelurida.com/ (last visited Feb. 6, 2021). Jelurida is a blockchain software company that develops and maintains the Nxt and Ardor blockchains. *See https://www.jelurida.com/nxt; https://www.jelurida.com/ardor.*

[27] MakerDAO, https://makerdao.com/en/ (last visited Feb. 6, 2021). MakerDAO is owned by the Maker Foundation. The Maker Foundation is tasked with bootstrapping MakerDAO to fuel growth and drive the organization toward complete decentralization. While the Foundation provided development support through the launch of the cryptocurrency called Multi-Collateral Dai (MCD), it is currently spearheading efforts to decentralize development.

[28] Moloch DAO, https://www.molochdao.com/ (last visited Feb. 6, 2021).

generation of DAOs.[29] This type of automation is expected to increase the number of DAOs, so lawyers should expect to encounter DAO-related legal questions for investors and developers alike.

"As self-executing software running on a distributed blockchain, a DAO need not have any owners in the traditional sense. It simply operates and interacts with the world according to its algorithms."[30] Thus, while a DAO may have human creators, DAOs do not require human employees (or owners), which is a novel concept (and problem) for most jurisdictions. The direction or management of the DAO is typically done in two fashions: algorithmic and AI-assisted. The two fashions are not exclusive, however. Most DAOs are actually hybrids, with some aspects of management being hard-coded in an algorithm, while others are run by AI-trained neural networks. Still other DAOs employ machine learning algorithms to respond to changes in the market. In other words, the DAO can learn "on the job," based on its own perceived experience.

While hard-coded DAOs are eminently predictable in their behavior, their machine learning cousins are not. The predictability (or lack thereof) of DAOs has legal implications. Moreover, the risks (legal and otherwise) of DAOs, while manageable, entail the need for legal advice for investors. Consequently, lawyers need to be conversant in the technology of DAOs in order to advise their clients of the attendant legal implications. No case better illustrates this need for legal *and* technological acumen than one of the first DAOs (confusing called "*The DAO*"), which resulted in the infamous Ethereum DAO attack.

"Up until it collapsed, The DAO represented the highest technological achievement – and the coming wave of innovation – that the Ethereum blockchain has enabled."[31] The DAO was the brainchild of Dan Larimer[32] and Vitalik Buterin,[33] the latter being a Russian-Canadian programmer and co-founder of the Ethereum blockchain. The DAO was a crowdfunding service implemented on the Ethereum blockchain.

> "The DAO, which got that name for being the first encoded version of the concept, was the proving ground that the disruptive world of venture capitalism

---

[29] *See, e.g.,* Limited Liability DAOs, Github, https://github.com/dOrgTech/LL-DAO.

[30] Werbach, *supra* note 14, at 110.

[31] Daniel Kuhn, *Did Ethereum Learn Anything From the $55M DAO Attack?*, Coindesk (Sept. 20, 2020), https://www.coindesk.com/ethereum-learn-dao-attack.

[32] *See, e.g.,* Dan Larimer, Steem.Center, https://www.steem.center/index.php?title=Dan_Larimer.

[33] *See, e.g.,* Vitalik Buterin, WIKIPEDIA, https://en.wikipedia.org/wiki/Vitalik_Buterin.

could itself be disrupted. Approximately $150 million in ether was contributed to the project, and more than 50 projects were teed up to possibly be funded by a smart contract that no one person owned."[34]

Once created, The DAO was attacked. Hackers detected a vulnerability in the code making up The DAO and exploited it. They got away with millions of dollars in cryptocurrency. Worse, copycats appeared and even more cryptocurrency was lost. "Investors withdrew their funds, a 'dark DAO' was spun up to protect the remaining and a serious debate raged over when it might be appropriate to hard fork or roll back events on a blockchain."[35] In the aftermath, market exuberance and lack of attention to security were blamed for the fiasco. For the developer community, it was a hard lesson. Fortunately, the security issues were surmountable, so the overall assessment of the technology remained buoyant. For the investment community, The DAO debacle was an expensive lesson, and demonstrated the need to limit risk while the developers sorted out the details.

6. Business Organizations for Blockchain-Oriented Companies

Several states (such as Delaware[36]) expressly allow the use of blockchains for corporate functions within a standard corporation. However, entrepreneurs determined that a specialized business entity was needed to facilitate the development and implementation of DAOs. That need is particularly acute because DAOs can be fitted with artificial intelligence ("AI") that can – without human interaction – modify the DAO's business model, or develop other business models and pursue different business goals than were first envisioned by its human creators.[37] Because the developers and owners of the DAO cannot predict what the DAO's AI will do, they understandably wish to limit their liability while still being able to profit from the DAO.

---

[34] Kuhn, *supra* note 33.

[35] *Id.*

[36] *See, e.g.*, Wonnie Song, *Bullish On Blockchain: Examining Delaware's Approach to Distributed Ledger Technology in Corporate Governance Law and Beyond*, Harvard Bus. L. Rev. (2017), https://www.hblr.org//wp-content/uploads/sites/18/2018/01/Bullish-on-Blockchain-Examining-Delaware%E2%80%99s-Approach-to-Distributed-Ledger-Technology-in-Corporate-Governance-Law-and-Beyond.pdf.

[37] *See, e.g.,* Prashant Ram, *The implications of AI on the Blockchain*, Hackernoon (July 24, 2018), https://hackernoon.com/the-distributed-autonomous-organization-dao-and-how-blockchain-ai-can-take-over-the-network-17a51f099d0f. *But see,* Werbach, *supra* note 14, at 110 ("Trusting an AI-trained system, therefore, adds another degree of risk over trusting a system based on hard-coded algorithms.")

In 2018, Vermont became the first state to enact a specific business organization type in 2018, namely a blockchain-based L.L.C.[38] Another state, Wyoming,[39] is following Vermont's lead and has pending legislation tailored to companies making heavy (if not exclusive) use of blockchains.

7. Example: Vermont's BBLLC Statute

Vermont's blockchain-based limited liability corporation ("BBLLC") statute is under Title 11, §§ 4171-4176.[40] Essentially, the BBLLC is just a regular LLC with some added requirements that are peculiar to DAOs. The statutes state that the "BBLLC may provide for its governance, in whole or in part, through blockchain technology."[41] In Vermont, the company must specify, in its articles of incorporation, that it has elected to be a BBLLC,[42] and subsection (2) of § 4173 includes six other requirements:

(A) provide a summary description of the mission or purpose of the BBLLC;[43]

(B) specify whether the underlying blockchain "will be fully decentralized or partially decentralized" and whether the blockchain "will be fully or partially public or private, including the extent of participants' access to information and read and write permissions with respect to protocols;"[44]

(C) "adopt voting procedures, which may include smart contracts" that are implemented on the blockchain to address forking,[45] changes to the operating agreement of the BBLLC,[46] and "any other matter of governance or activities within the purpose of the BBLLC;"[47]

(D) "adopt protocols to respond to system security breaches or other unauthorized actions that affect the integrity of the blockchain technology utilized by the BBLLC;"[48]

---

[38] *See* VT. STAT. ANN. tit. 11, § 4173.

[39] *See*, Wyoming Senate Bill SF0038 (2021), https://wyoleg.gov/Legislation/2021/SF0038.

[40] VT. STAT. ANN. tit. 11, § 4171 *et. seq.*

[41] *Id.* § 4173(1).

[42] *Id.* § 4172.

[43] *Id.* § 4173(1)(A).

[44] *Id.* § 4173(1)(B).

[45] *Id.* § 4173(1)(C)(i).

[46] *Id.* § 4173(1)(C)(ii).

[47] *Id.* § 4173(1)(C)(iii).

[48] *Id.* § 4173(1)(D).

(E) "provide how a person becomes a member of the BBLLC with an interest, which may be denominated in the form of units, shares of capital stock, or other forms of ownership or profit interests;"[49] and

(F) "specify the rights and obligations of each group of participants within the BBLLC, including which participants shall be entitled to the rights and obligations of members and managers."[50]

The Vermont statute makes special mention of *members* and *managers*. However, those terms don't have any special meaning within the ambit of the BBLLC statute, and thus have the same meaning as for other LLCs. § 4174 expressly states that members and managers can have multiple roles within the BBLLC, "including as a member, manager, developer, node, miner, or other participant in the BBLLC, or as a trader and holder of the currency in its own account and for the account of others, provided such member or manager complies with any applicable fiduciary duties."[51] This remains true regardless of the location of that person.[52]

Finally, the Vermont BBLLC law has a very important provision regarding the technological structure of the company. § 4175 requires that, in the governance of the corporation, the company may "adopt any reasonable algorithmic means for accomplishing the consensus process for validating records, as well as requirements, processes, and procedures for conducting operations, or making organizational decisions on the blockchain technology used by the BBLLC."[53]

Clearly the authors of the Vermont BBLLC law were concerned, for investors' sake, about the design of the blockchain, as reflected in subsections (B), (C) and (D). It should be noted, however, that Vermont law did not directly affect the potential of AI morphing the operation of the DAO. However, Vermont made a very clever caveat provision that should apply in situations with AI-in-command, namely § 4175(2), which requires "in accordance with any procedure specified pursuant to section 4173 of this title, modify the consensus process, requirements, processes, and procedures, or substitute a new consensus process, requirements, processes, or procedures that comply with the requirements of law and the governance provisions of the BBLLC."[54] In other words, if the AI (or humans) morph the company's business model and/or

---

[49] *Id.* § 4173(1)(E).
[50] *Id.* § 4173(1)(F).
[51] *Id.* § 4174(a).
[52] *Id.* § 4174(b).
[53] *Id.* § 4175(1).
[54] *Id.* § 4175(2).

governance model, an amendment to the articles of incorporation is required. In any case, lawyers who are going to advise clients as to *how* to characterize the blockchain and operation, as required in subsections (B), (C) and (D) of § 4173, will need to be versed in the technology.

Wyoming's proposed legislation, SF 38,[55] differs from Vermont's law. Under SF 38, the company is an LLC that elects a "status" as a "decentralized autonomous organization." Unlike Vermont, a Wyoming company that is already an LLC could (under the proposed legislation) "convert" to claim DAO status by amending its articles of organization to include the required language.[56] Interestingly, SF 38 requires that the status of the DAO be included within the name of the company in one of three ways: "DAO", "LAO", or "DAO LLC."[57] Another important requirement in SF 38 is that a DAO must, within the articles of incorporation, define the company as *either* a member managed DAO, or an algorithmically managed DAO (and the member managed selection is the default).[58]

There are some additional requirements under Wyoming SF 38, namely the requirement that "the articles of organization shall include a publicly available identifier of any smart contract directly used to manage, facilitate or operate the decentralized autonomous organization."[59] How that would work in practice is an open question. As alluded to with the Vermont law, the Wyoming legislation would require amendment of the articles of incorporation if the DAO's smart contracts are "updated or changed."[60] Presumably, that change could be accomplished by a human or by AI-enhanced code, although the proposed legislation was silent as to that issue.

8. Conclusion

Distributed autonomous organizations exist and are here to stay. Their profit potential is obvious and substantial, particularly because smart contracts and DAOs can reduce transaction costs. However, DAOs are not without risk, and the need to limit liability is necessary for the potential of DAOs to be realized. States are beginning to tailor specialized business entities that address the particular concerns of DAOs. While the technology and business models for DAOs are evolving rapidly, the statutory schemes are also going to change, albeit at a slower and delayed pace than the technology. Even so, some companies are taking advantage of

---

[55] Wyoming Senate Bill SF0038 (2021), https://wyoleg.gov/Legislation/2021/SF0038.

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*

particularized corporate forms, and other states will likely follow Vermont's lead in order for those states to remain competitive.

About the Author

Ronald Chichester is a solo attorney who is a past chair of the Business Law Section and a past chair of the Computer & Technology Section of the State Bar of Texas. His area of practice includes computer torts and computer crimes.

Appellate Concerns About Zoom Trials

By Judge Emily Miskel

During the pandemic, courts have remotely held trials and hearings of all kind, using videoconferencing software like Zoom. Attorneys have concerns about how the new technology might affect a trial record or an appeal. This article lists some common remote hearing issues that can affect a trial court record.

A. Inaudible Audio

Videoconferencing connection quality varies widely. Court reporters' records can frequently contain instances of "inaudible," "unintelligible," or "audio disruption." There are a few options that parties or a court can take if a critical word was missed or misheard in the reporter's record.

Tex. R. App. P. 34.6(e) governs inaccuracies in the reporter's record. Inaccuracies may be corrected by agreement of the parties,[1] or, with notice and hearing, the trial court can correct the inaccuracy.[2] Given that trial courts in Texas dispose of dozens of cases each week, such a hearing should be set as quickly as possible in order to improve the chances that the trial court may recall the testimony. If the dispute arises after the reporter's record has been filed in an appellate court, the court may submit the dispute to the trial court to resolve.

B. Corrupted Electronic Exhibits

Appellate lawyers may also fear that an electronic exhibit becomes corrupted or inaccessible. Tex. R. App. P. 34.6(f) provides guidance when a portion of the reporter's record is lost or destroyed. A new trial can be avoided if the lost, destroyed, or inaudible portion of the reporter's record can be replaced by agreement of the parties or with a copy determined by the trial court to accurately duplicate with reasonable certainty the original exhibit.[3] Even in traditional in-person trials, an attorney or witness will occasionally leave the courthouse with an original exhibit. Generally, the court will have everyone back on the record to substitute a copy of the exhibit. Similarly, if an electronic exhibit was published at trial, and the court reporter later discovers that her copy is corrupted, the exhibit can be replaced with a duplicate.

---

1 Tex. R. App. P. 34.6(e)(1).

2 *Id.* § 34.6(e)(2).

3 *See id.* § 34.6(f)(4).

C. Access to Video or Audio Recordings of Trial

Now that audio and video recordings of trials exist, parties are naturally curious about how they can obtain and use them. States handle trial video recordings differently, but under current Texas rules, you are unlikely to be able to obtain video or audio trial recordings.

Parties cannot compel a court to produce the court's copy of trial recordings. Rule 12 of the Texas Rules of Judicial Administration governs Public Access to Judicial Records. The rule contains procedures for requesting judicial records from courts. However, the definition of "judicial record" expressly excludes any record that relates to a matter that has been before a court: "Judicial record means a record made or maintained by or for a court or judicial agency in its regular course of business but not pertaining to its adjudicative function, regardless of whether that function relates to a specific case. A record of any nature created, produced, or filed in connection with any matter that is or has been before a court is not a judicial record."[4] Therefore, parties do not have the ability to compel a court to preserve or produce any audio or video recording that a court makes of a hearing or trial.

Parties are generally prohibited from recording their own copies of court proceedings. Many trial courts are providing public access to court proceedings by live-streaming the proceedings online. Courts do not have technical tools to prohibit observers from making their own copies of the streaming video. However, many courts put a "do not record" watermark on the video and make admonishments that parties are not to record. Tex. R. Civ. P. 18c implies that recordings may only be made if permitted by the trial court, and it is common practice in trial courtrooms to prohibit parties from recording court proceedings.

Further, under Tex. R. App. P. 34.1, "[t]he appellate record consists of the clerk's record and, if necessary to the appeal, the reporter's record."[5] Therefore, the extra audio or video recordings of a trial are not part of the appellate record.

D. Exhibits Displayed but not Admitted into Evidence

Sometimes a video trial can feel more informal than an in-person trial. Parties may refer to evidence that hasn't been admitted, screenshare documents, hold up notes, or try to play recordings that are not in evidence. The trial attorney should ensure a clear record by objecting to anyone publishing or referring to evidence that has not been admitted.

---

4 Tex. R. Jud. Admin. 12.2(d).

5 Tex. R. App. P. 34.1.

E. Physical Evidence

While most documents and recordings can be submitted in electronic format, some exhibits exist only in physical form. If a party needed to use an object as an exhibit in a remote trial, the party could arrange to pre-mark the object and deliver it to the court in advance of the remote trial. Then, during the remote proceeding, the parties would likely work with photos or videos of the object.

F. Sensitive Data and Trade Secrets

Exhibits admitted into evidence have always been open to the public. Frequently, in traditional court proceedings, parties will offer exhibits that contain social security numbers, bank account numbers, and other information that is confidential or sensitive. Now, with livestreaming on YouTube, parties are realizing how public their court documents are. Attorneys should carefully redact private client information before admitting it into evidence in a public proceeding.

Tex. R. Civ. P. 21c(b) prohibits filing documents that contain sensitive data in the clerk's record, unless the inclusion of sensitive data is specifically required by statute, court rule, or administrative regulation. Absent such requirement, documents containing sensitive data may not be filed with a court unless the sensitive data is redacted.[6] If a party discovers that a document has been filed that contains sensitive data, the clerk may accept a redacted substitute copy and the court can order that a party submit a redacted substitute copy to the clerk.[7] Tex. R. Civ. P. 21c has been held to apply to the clerk's record but not the reporter's record.[8]

In traditional, in-person court proceedings, parties can request to seal portions of a reporter's record that contains trade secrets.[9] With video hearings, parties should additionally request that the court stop any public livestreaming of the proceeding if trade secrets will be discussed.

G. Disconnection

It is not uncommon for someone's connection to fail during a video trial. If an attorney notices that someone has dropped off the video call, she should ask for the hearing to be paused until

---

6 Tex. R. Civ. P. 21c(c).

7 *See id.* § 21c(e).

8 *See*, *e.g.*, *In re Srivastava*, No. 05-17-00998-CV, 2018 WL 833376, at *4 (Tex.App.—Dallas Feb. 12, 2018) (mem. op.).

9 *See*, *e.g.*, *In re MI LLC*, 505 S.W.3d 569, 578 (Tex. 2016).

that person can rejoin. If the judge is the one who is dropped from the call, the parties should remain calm, pause, and wait for the judge to rejoin.

H. Admonishments and Standing Orders

Many courts have written Zoom hearing instructions, detailed standing orders for remote hearings, or specific admonishments relating to some of these problems. If attorneys have specific concerns, they should ask the court to make a specific admonishment.

It is also important to review all of the trial court's new procedures and orders before trial. For example, some courts require exhibits to be exchanged electronically by noon the day before the hearing, while other courts will accept exhibits the same day as the hearing. Trial lawyers would not want important evidence to be excluded because they did not exchange it timely under the court's emergency remote-hearing policy.

In a recent case, a party mandamused the trial court for refusing to rule on her motion to hold a pretrial hearing on Zoom.[10] The appellate court denied the mandamus, noting that the court had a standing order with specific procedures to request a video proceeding, requiring a party to provide an email address and submit exhibits electronically.[11] The party did not show that she complied with the procedure in the standing order or that the trial court refused to follow the procedure.

I. Conclusion

Remote video trials may seem strange, and it is always hard to adapt to something new. However, there is generally a solution for every problem. Attorneys should be ready to speak up promptly if there is a concern and ideally offer the court a proposed solution.

About the Author

Judge Emily Miskel of the 470th district court of Collin County, Texas, was appointed by Gov. Greg Abbott in 2015. She is board certified in family law by the Texas Board of Legal Specialization. Judge Miskel has an engineering degree from Stanford University, and she received her law degree from Harvard Law School. Before she was judge of the 470th district court, she practiced family law in Plano, Texas.

[10] *In re Ward*, No. 09-20-00186-CV, 2020 WL 4218225, at *1 (Tex.App.—Beaumont Jul. 23, 2020) (mem. op.).

[11] *Id.*

Feeling that Livestreamed Pain: Virtual Bystander Recovery

By John G. Browning

The doctrine of bystander recovery—allowing the recovery of emotional distress damages for someone who suffered as a result of witnessing the injury or death of a close relative—was first ushered into American common law over fifty years ago by the California Supreme Court in its landmark decision in *Dillon v. Legg*.[1] So perhaps it comes as no surprise that the first court to recognize a cause of action for *virtually* witnessing physical harm to or the death of a family member would also be a California appellate court. In a late December opinion in *Dyana Ko, et al. v. Maxim Healthcare Services, Inc.*, the California Court of Appeals (Second Appellate District) held that a California couple could maintain claims of negligence and negligent infliction of emotional distress against the employer of a vocational nurse who had abused the couple's disabled son—even though they witnessed the abuse via livestream of video and audio on Dyana Ko's smartphone from a "nanny cam" in the home.[2]

The case may very well be appealed to the California Supreme Court. But in an era in which Americans consume news, sports, and entertainment on their smartphones, and where even in pre-pandemic conditions, virtual interactions have become a staple of everyday life, can we honestly say that witnessing a traumatic event in real time virtually is less impactful than witnessing it "in real life," i.e., being physically present at the scene? In the Digital Age, people have committed shocking acts via livestreaming apps like Facebook Live, including mass shootings, murder, sexual assault, torture, and suicide. Who can say that witnessing such an incident involving a family member is any less visceral if the viewing is enabled by technology rather than physical presence? To fully appreciate what could be a seismic shift in tort law, it is necessary to understand more not only about the *Ko* case itself, but also its context among the cases construing the *Dillon v. Legg* bystander recovery doctrine, and what effect might eventually be felt in Texas bystander recovery cases.

I. THE NANNY CAM REVEALS ALL

On April 22, 2017, Dyana and Khristopher Ko took their two older children to a youth basketball tournament. Their youngest child, two-year-old Landon, was at home under the care of Thelma Manalastas, a nurse from Maxim Healthcare Services who had been one of Landon's full-time caregivers for over a year. Landon had a genetic disorder, Rubinstein-Taybi

---

[1] 68 Cal. 2d 728 (1968).

[2] *Ko v. Maxim Healthcare Servs., Inc.*, 58 Cal. Ct. App. 5th 1144, 1149 (Dec. 23, 2020).

Syndrome, that caused him to suffer a myriad of health problems, including blindness in one eye, an inability to walk, difficulty hearing, the need for a feeding tube, and severe developmental delays. While at the basketball tournament, Dyana Ko "opened a phone application that allows her to live-stream video and audio from her home that is being shot in real time on a 'nanny cam.'"[3] According to the Kos' complaint, the parents "watched and heard in shock and horror while the incident was happening in real time, as . . . Manalastas physically assaulted Landon by acts including hitting, slapping, pinching, and shaking Landon in a violent manner."[4] The Kos called 911, police were dispatched to their residence, and when the couple arrived, they showed the police the video of the abuse. Manalastas was arrested. The Kos reported the abuse to Maxim, which reassigned Manalastas instead of firing her.[5]

The Kos filed a lawsuit against Manalastas and Maxim on June 21, 2017.[6] They asserted claims for negligence, battery, assault, and negligent infliction of emotional distress (NIED). Landon had suffered various physical injuries, necessitating the surgical removal of one of his eyes. On April 24, 2018, while the lawsuit was still pending, Landon passed away. Defendants Maxim and Manalastas filed demurrers to the Kos' claims for NIED. The trial court sustained the demurrers, noting that under existing California case law, "NIED bystander liability is limited to circumstances where a plaintiff is physically 'present at the scene of the injury producing event at the time it occurs.'"[7] The court observed that cases upholding NIED liability had only involved plaintiffs with some physical proximity to the injury-producing event, even though appellate courts had never defined what it means to be "present at the scene."[8] The trial court went on to say, "It is unclear how existing case law on NIED applies to existing technology, such as live-streaming video and audio on smart phones".[9]

II. THE DECISION

On appeal, the California Court of Appeals began with a historical overview of the 1968 case of *Dillon v. Legg* and its progeny. In *Dillon*, the California Supreme Court held that a mother could recover for the emotional shock and physical injury resulting from seeing her young daughter run over by the defendant, when she was in close proximity to the collision but not in the

---

3 *Id.* at 1147.
4 *Id.*
5 *Id.* at 1148.
6 *Id.*
7 *Id.*
8 *Id.*
9 *Id.*

"zone of danger" herself.[10] Responding to concerns about "potentially infinite liability" for bystander NIED claims, the *Dillon* court pronounced three factors that would help determine the elements of foreseeability in such cases: (1) whether the plaintiff was located near the scene of the incident; (2) whether the shock resulted from a direct emotional impact stemming from sensory and contemporaneous observance of the incident (as opposed to learning of it from others); and (3) whether the plaintiff and victim were closely related.[11]

In the decades that followed, the California Supreme Court and various courts of appeal expanded the bystander recovery doctrine, recognizing viable NIED claims in a variety of circumstances. In a case in which the husband was present, but did not see his wife struck and killed while unloading groceries from the family car, the court said a visual perception was not necessary, as long as there were other sensory, contemporaneous observances.[12] It later allowed claims that did not involve a sudden occurrence, as in the NIED claims of a mother who watched her son suffer excruciating pain over several days before dying.[13] Other decisions relaxed the "contemporaneous" prong, allowing NIED claims to proceed where a parent came upon the scene of the accident within moments.[14] But beginning with its decision in *Thing v. La Chusa*, the California Supreme Court pulled back from this expansion, holding that a bystander plaintiff must be present at the scene of the injury-producing event at the time it occurs.[15]

Following *Thing*, subsequent decisions rejected the NIED claims of daughters whose mother's artery was cut during surgery, because they were not present in the operating room;[16] of a wife who heard (but did not see) the sound of a sign falling on her husband's head;[17] and of a scuba diver's sister who witnessed his death during a dive but did not know it was due to defective equipment.[18] However, the *Ko* court pointed out the changes in live television and remote video surveillance that have taken place. Acknowledging the "ubiquity of home

---

[10] *Dillon v. Legg*, 68 Cal. 2d 728, 748 (1968).

[11] *Id.* at 740–41.

[12] *Krouse v. Graham*, 19 Cal. 3d 59, 76 (1977).

[13] *Ochoa v. Superior Court*, 39 Cal. 3d 159, 167 (1985).

[14] *See, e.g.*, *Archibald v. Braverman*, 275 Cal. App. 2d 253 (1969) (mother did not witness explosion, but was on scene within moments to aid son); *Nazaroft v. Superior Court*, 80 Cal. App. 3d 522, 533 (1978) (mother did not witness three year-old son's drowning, but arrived as he was being pulled from the pool).

[15] 48 Cal. 3d 644, 668 (1989).

[16] *Bird v. Saenz*, 28 Cal. 4th 910 (2002).

[17] *Ra v. Superior Court*, 154 Cal. App. 4th 142 (2007).

[18] *Fortman v. Förvaltningsbolaget Insulan AB*, 212 Cal. App. 4th 830 (2013).

surveillance systems and videoconferencing applications," the court noted how "the advent of Internet-enabled smartphones has manifestly changed the manner in which families spend time together and monitor their children."[19] Observing that courts are often "called upon to interpret longstanding precedent in light of new technologies",[20] the court held that the Kos could maintain a cause of action for NIED because they "were virtually present through modern technology that streamed the audio and video on which they watched Manalastas assaulting Landon in real time," and thus they personally and contemporaneously perceived the injury-producing event and its traumatic consequences.[21]

III. WHAT NEXT?

Could other courts hold that such technology-aided contemporaneous perception will satisfy the criteria for bystander recovery claims? Will an individual who witnesses a close relative's injury or death on Facebook Live, for example, be able to assert such claims? Or perhaps a person at work, who witnesses the death of a spouse via Ring doorbell camera or other home surveillance technology? The Indiana Supreme Court held in 2015 that a plaintiff father could not recover for NIED where he watched a television news story about a fatal car crash near his home and feared his son was involved.[22] To date, however, even among the few tort cases involving livestreaming applications, such bystander recovery claims have not been raised.[23]

And how about Texas? Texas does recognize recovery for a bystander's NIED claims, provided that the bystander was located near the scene of the accident; suffered shock as a result of "a direct emotional impact . . . from a sensory and contemporaneous observance of the accident"; and that the bystander and the victim were closely related.[24] Texas law recognizes that the elements of a bystander claim are "flexible," and applied on a case-by-case basis.[25] To show contemporaneous perception, Texas courts require that the bystander show that she either witnessed the accident or experienced the shock of unwittingly coming upon the accident scene. For example, a mother who did not see or hear the crash that occurred a block away

---

[19] *Ko*,58 Cal. Ct. App. At 1158.

[20] *Id.*

[21] *Id.* at 1159.

[22] Clifton v. McCormack, 43 N.E.3d 213 (2015).

[23] *See, e.g.*, *Maynard v. Snapchat*, 358 Ga. App. 496, 503 (Oct. 30, 2020) (a divided Georgia appellate court upheld the trial court's dismissal of a plaintiff's product liability claims that messaging app Snapchat's "Speed Filter" was to blame for a wreck after a teenage driver tried to record herself driving 100 miles an hour).

[24] *United Servs. Auto. Ass'n v. Keith*, 970 S.W.2d 540, 541-42 (Tex. 1998).

[25] *Id.* at 542.

was not considered "at the scene."[26] Similarly, a father who was a half-mile away from where his son was shot was not "near the scene."[27] However, a father who found his son dead at the bottom of a hospital's airshaft after a three-hour search for him in the facility was deemed to be at the scene with contemporaneous perception.[28]

Given that directive for Texas courts to be flexible and consider bystander recovery claims on a case-by-case basis, and recognizing that technology issues are continuing to impact courts' consideration of everything from service of process to evidence to personal jurisdiction to contract formation and interpretation, it would not be surprising to see a Texas court issue a ruling similar to the *Ko* court. After all, products like Amazon's Ring and Google's Nest have dominated the smart home market, with experts estimating that as of early 2020, more than twenty million homes in the U.S. have a video doorbell. The technology making our virtual monitoring in real time is here to stay, and our jurisprudence needs to catch up with it.

About the Author

John G. 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.

[26] *Id.*

[27] *Lehmann v. Wieghat*, 917 S.W.2d 379, 384 (Tex. App.—Houston [14th Dist.] 1996, writ denied).

[28] *City of Austin v. Davis*, 693 S.W.2d 31, 34 (Tex. App.—Austin 1985, writ ref'd n.r.e.).

eDiscovery – Examples from Recent Cases

By Judge Emily Miskel

Much relevant discovery is now stored electronically, and requesting parties frequently have concerns about whether responding parties are producing all responsive data. Several recent cases give guidance on when and how a party can compel direct access to electronically stored information, including cloud storage, database information, and social media evidence.

A. Cloud Data

Many cases involving direct access have dealt with physical devices such as hard drives or backup tapes. A recent decision extends the direct access holdings of *Weekley Homes*[1] to cloud data.[2] In the case, a medical practice sued two doctors for claims relating to trade secrets and patient relationships. The practice sought forensic analysis of the doctors' electronic practice management systems to determine revenues generated by the two doctors and the patients they referred.[3]

The plaintiff argued that the standards in *Weekley Homes* did not apply, because it was not seeking access to any electronic storage device. Rather, the electronic practice management system was a web-based service that required no installation on the new practice's devices.

The appellate court held that the distinction was not relevant.[4] The court iterated that *Weekley Homes* "did not focus on the technical details of how, or where, a party stores its data; it focused instead on addressing undue burden and placing specific limits on a highly intrusive form of discovery involving direct access to one litigant's data by a litigation opponent or an expert paid by the opponent. The . . . intrusion concerns apply regardless of whether the responding party stores its data on a hard drive in its possession or instead stores its data in a database that can be accessed remotely. The focus is access to data and the circumstances under which access will be allowed."

---

1 *In re Weekley Homes, L.P.*, 295 S.W.3d 309 (Tex. 2009).

2 *In re Methodist Primary Care Grp.*, 553 S.W.3d 709, 718–19 (Tex. App.—Houston [14th Dist.] 2018).

3 *Id.* at 712.

4 *Id.* at 718.

B. Specifying Search Terms may be Direct Access

The recent *Master Flo* case held that a trial court's order for a company to search its email systems and electronic files using keywords supplied by the court was akin to direct access to the storage devices, and the *Weekley Homes* requirements applied.[5] The court noted that "[a]n order that a party conduct certain keyword searches of its electronic files intrudes on a party's right to develop its own means of searching for responsive documents without court involvement or interference by the opposing party."[6] Without evidence that a party has failed to adequately search for responsive documents, "a trial court should not be involved in managing how a party performs searches of its electronic data for responsive documents."[7] The court held that the requesting party did not meet its threshold burden to show that the responding party defaulted on its discovery obligations, and so was not entitled to dictate search terms.[8]

However, another recent case held that seeking database listings, tables of contents, or indexes is not improper and does not amount to direct access.[9] That trial court's order compelled the defendant to:

- Provide a listing or table of contents sufficient to identify the folders and sub-folders within specified databases,
- Provide a copy of the index from which the papers maintained in its technical library can be identified,
- Conduct additional searches in accordance with a protocol to formulate appropriate search queries,
- Produce documentation showing the search queries that were performed and describe the results generated to enable the plaintiffs to determine whether search modifications should be made, and
- Determine whether documents should be withheld from production based on a privilege, before allowing the plaintiffs to review the responsive documents.[10]

The defendant objected that the order was overbroad and allowed the plaintiffs to pursue what amounts to direct access to its databases, in violation of *Weekley Homes*. The Dallas court of

---

5 *In re Master Flo Valve Inc.*, 485 S.W.3d 207, 220 (Tex. App.—Houston [14th Dist.] 2016).

6 *Id.*

7 *Id.*

8 *Id.* at 220-21.

9 *In re Toyota Motor Sales, U.S.A., Inc.*, No. 05-18-00582-CV, 2018 Tex. App. LEXIS 4395 at *9 (Tex.App.—Dallas [5th Dist.] June 14, 2018).

10 *Id.* at *7-*8.

appeals specifically declined to follow *Master Flo* and held that providing information about databases and libraries is not direct access.[11] Further, *Weekley Homes* directs litigants to cooperate in formulating search results and in sharing the results, and does not require a showing of discovery default for that. However, the court held that portions of the trial court's order were overbroad and should have been more tailored to timeframes and subject matters related to the case.[12]

C. Social Media

As social media evidence became more commonly used in trials, attorneys were naturally skeptical that the opposing party would produce all the information requested in discovery. It was commonplace for attorneys to file motions to compel, requesting that the opposing party turn over a login and password so that the social media discovery could be directly obtained. As discussed in *Weekley Homes* and *Shipman*, Texas law discourages direct access to an opposing party's data.[13]

Once it became more commonly known that it was improper to request direct login information, parties began crafting production requests for the opposing party to download an archive of an entire social media account and produce the complete archive in discovery. Discovery requests cannot be fishing expeditions in hopes of finding impeachment evidence and must be reasonably tailored to include only matters relevant to the case.

As described in *Shipman*, suspicion that a party has not produced everything is not evidence of discovery abuse.[14] In the Texas litigation system, parties must rely on the opposing party to review and produce what has been requested. Without evidence that a party has defaulted on her obligations to search her records or evidence that her production was inadequate, it is an abuse of discretion to allow direct access to social media data.[15] A party seeking discovery must propound a properly tailored request and allow the opposing party to review and produce responsive material.

---

[11] *Id.* at *9.

[12] *Id.* at *11.

[13] *See In re Weekley Homes*, 295 S.W.3d; *In re Shipman*, 540 S.W.3d 562 (Tex. 2018) (per curiam).

[14] *See In re Shipman*, 540 S.W.3d at 565.

[15] *See id.*

About the Author

Judge Emily Miskel of the 470th district court of Collin County, Texas, was appointed by Gov. Greg Abbott in 2015. She is board certified in family law by the Texas Board of Legal Specialization. Judge Miskel has an engineering degree from Stanford University, and she received her law degree from Harvard Law School. Before she was judge of the 470th district court, she practiced family law in Plano, Texas.

Personhood and Technology

By John G. Browning

In the oft-criticized decision in *Citizens United v. Federal Elections Commission*, the U.S. Supreme Court held that corporations (including nonprofits, labor unions, and other business entities) had a First Amendment right to engage in political communications.[1] Yet in April 2020, the U.S. Patent & Trademark Office (USPTO) ruled that an application listing an artificial intelligence system (the Device for the Autonomous Bootstrapping of Unified Sentence, or "DABUS") as the inventor was incomplete because it failed to identify a human inventor. In its decision,[2] the USPTO cited certain Federal Circuit precedent stating that only natural persons can be inventors.[3] But putting aside these seemingly at-odds legal interpretations of personhood when it comes to free speech or intellectual property rights, can a computer be considered a "person" in the eyes of the law for other purposes, such as the question of what constitutes hearsay?

That's the novel question at the heart of a recent Arizona appellate decision, *Stuebe v. Arizona*, in which the court considered whether a computer-generated video notification should be considered hearsay.[4] In February 2018, police in Maricopa County, Arizona responded to a 911 call from a security company prompted by a silent alarm at a Glendale commercial property. Police stopped a fleeing SUV, in which Jerry Stuebe was a passenger; the vehicle also contained two bags which held burglary tools, copper wire, and boltcutters. The building's property manager testified that he had received a computer-generated email from the security company after a motion-sensor security camera was activated; attached to the email was a video file incriminating Stuebe, and the email specified the date and time of the video. The email and video were admitted over Stuebe's objection, and he was convicted of third-degree burglary and sentenced to ten years in prison.[5]

Stuebe appealed, arguing that the email and video were inadmissible hearsay, and that his Sixth Amendment rights under the Confrontation Clause had been violated. Arizona, like many states, models its evidence rules after the Federal Rules. Both apply to a "person's" statements

---

1 558 U.S. 310 (2010).

2 Decision on Petition, *In re* Application of No. 16/524.350 (2020).

3 *Univ. of Utah v. Max-Planck-Gesellschaft zur Forderung der Wissenschaften E.V.*, 734 F.3d 1315, 1323 (Fed. Cir. 2013).

4 467 P.3d 252 (Ariz. Ct. App. Jun. 30, 2020).

5 *Id.* at 254.

and "the person who made the statement" in considering the rule against hearsay. But because there is not set definition of "person" in the Rules of Evidence, the appellate court interpreted the word according to its common definition—which does not include a computer or other machine.[6] Thus, the court held that the email and video were not statements by a "person" but were "machine produced" and accordingly could not be classified as hearsay.[7] With the evidence found to be admissible, the conviction was affirmed.

This is consistent with how federal courts have generally held, reasoning that computer results are not hearsay. In *United States v. Lizarraga-Tirado*, for example, the Ninth Circuit ruled in 2015 that GPS tracking does not constitute hearsay.[8] The court reasoned that the satellite image, much like a photograph, makes no assertion and therefore cannot be hearsay. However, the court conceded that when Google Earth GPS puts a marker or tack at the coordinates, the issue becomes thornier. Noting that "labeled markers added to a satellite image do make clear assertions", the court observed that a tack placed manually would be hearsay while an automatically-placed tack would not.[9] Other courts have reached similar conclusions that "machine statements" by computers are not hearsay. This includes telephone billing records,[10] machine-generated medical laboratory results,[11] and computer-generated date and IP address data headers in photographs.[12]

But as computers increasingly take on tasks more traditionally performed by humans, this legal question becomes more complicated. Artificial intelligence is playing an increasingly important role in the practice of law (including drafting of pleadings and reviewing/drafting contracts). And for years, lawyers have depended on computerized legal research and e-Discovery related document review. In 2013, document review attorney David Lola sued a large law firm and a legal staffing provider for overtime wage violations, igniting a debate over whether such technology-assisted document review constituted the practice of law, and whether e-Discovery review lawyers fell under the regulatory exemptions for licensed attorneys engaged in the practice of law. The case went all the way to the Second Circuit in 2015, which held that (under

---

6 *Id.* at 255-56.

7 *Id.* at 256.

8 789 F.3d 1107 (9th Cir. 2015).

9 *Id.* at 1109.

10 *United States v. Lamons*, 532 F.3d 1251 (11th Cir. 2008).

11 *United States v. Moon*, 512 F.3d 359 (7th Cir. 2008).

12 *United States v. Hamilton*, 413 F.3d 1138 (10th Cir. 2005).

North Carolina law), the e-Discovery document review done by Lola and others did not constitute the practice of law.[13]

Some legal scholars point out that as technology causes the number of "witnesses" immune to cross-examination to rise—citing DNA results and breathalyzers, among others—we should be more concerned about judicial rejection of a way to hold computers accountable. As Prof. Barry Sites says of such "machine accusers," computers are the creation of imperfect humans, which in turn render them imperfect.[14] Just as organic (human) sources of testimony can suffer from "hearsay dangers" like insincerity, ambiguity, memory loss, or misperception, machine sources can potentially suffer from "black box" dangers that can lead to a finder of fact drawing an incorrect inference from information conveyed by a machine. While it might not exhibit memory loss or dishonesty, a machine's programming can lead to its output being imprecise or false, thanks to human error in programming. For example, AI can exhibit bias if the developers of its algorithm incorporate such bias (consciously or unconsciously).

As technology marches on at a pace far beyond that of our jurisprudence, we may have to re-evaluate many of our long-held evidentiary arguments.

About the Author

John G. 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.

[13] *Lola v. Skadden, Arps, Slate, Meagher & Flom LLP*, 620 Fed. Appx. 37 (2d Cir. 2015).

[14] Brian Sites, *Machines Ascendant: Robots and the Rules of Evidence*, 3 GEO. L. TECH. REV. 1 (2018).

Cyberstalking Legislation Cannot Stifle Free Speech

By Pierre Grosdidier

Cyberstalking statutes seek to prevent and sanction the spectrum of mischief that occurs online, from school cyberbullying to sextortion. Cyberstalking can result in tragedy, as when ensnared and despairing teens commit suicide.[1] These statutes must nonetheless strike a balance between stifling criminal conduct and respecting free speech. Recently, in *United States v. Cook*, a United States District Court held that the federal cyberstalking statute was unconstitutional as applied because it failed the First Amendment's strict scrutiny test.[2] The decision is noteworthy because in *United States v. Conlan*, the Fifth Circuit Court of Appeals rejected a constitutional vagueness challenge to the prior (2006) version of the statute.[3]

The State of Mississippi unsuccessfully prosecuted Christopher Cook on drug charges. Cook voiced his grievances against authorities in a series of scornful Facebook posts, which formed the basis of federal Internet harassment charges under 18 U.S.C. § 2261A(2), the federal cyberstalking statute. The 2013 version of this statute, which applies in this case, states in part that

> [w]hoever— . . .
> (2) "with the intent to kill, injure, harass, intimidate, . . . , uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, . . . to engage in a course of conduct that— . . .
> (B) causes, *attempts to cause, or would reasonably be expected to cause substantial emotional distress* to [another person shall be punished]".[4]

---

1 *See, e.g.*, Joey L. Blanch and Wesley L. Hsu, *An Introduction to Violent Crime on the Internet*, 64 U.S. Attorneys' Bulletin 2, 3 (May 2016); Sarah Jameson, *Cyberharassment: Striking a Balance Between Free Speech and Privacy*, 17 CommLaw Conspectus 231, 232 (2008) (relating specific cases of teen suicide over sextortion and harassment, respectively).

2 472 F. Supp. 3d 326, 340 (N.D. Miss. 2020).

3 786 F.3d 380, 386 (5th Cir. 2015) (affirming conviction for, *inter alia*, sending victim threatening electronic correspondence); *but see*, *United States v. Cassidy*, 814 F. Supp. 2d 574, 588 (D. Md. 2011) (holding 2006 version of § 2261A(2)(A) unconstitutional as applied to objectionable Internet speech for failing to satisfy strict and intermediate scrutiny tests).

4 18 U.S.C. § 2261A(2) (2013) (emphases added). *Cook*'s holding should also apply to the current (2018) version of the statute.

On his personal Facebook page, Cook demeaned prosecutors, judges, and public defenders, and ominously warned that "you are finished. Because I'm coming and hell is coming with me. And I'm not just quoting a movie."[5] In another post, Cook revealed what appeared to be personal information of a state narcotics officer. In a final lengthy post, Cook decried an allegedly thoroughly corrupt indictment scheme and professed that "[n]ow for me it's war. I'm sick of the corruption in this state. . . . It's a mess and the people turn a blind eye here."[6] And, in reference to the officer and his family members, "God willing I'm going to take them out."[7]

As a threshold issue, the court noted that the government did not allege that Cook ever contacted the persons he berated, and that the indictment "cherry picked" and shuffled the statements in the posts to make them feel more ominous.[8] The court also held that the charges applied to the substance of Cook's posts, *i.e.*, his speech, not his "act of posting" or conduct. The point is important because § 2261A(2)(B) regulates conduct.[9]

The First Amendment protects speech, even if unpalatable or outrageous, and especially when it touches on public affairs. One of the narrow exceptions to this free speech rule are "true threats."[10] In the Fifth Circuit, a true threat is one that "in its context would have a reasonable tendency to create apprehension that its originator will act according to its tenor." True threats must have "immediacy, or clarity of purpose," and the threat recipient must "reasonably fear it would be carried out."[11]

Comparing Cook's conduct to that of other defendants in the Fifth Circuit, the court concluded that his posts were not true threats because they lacked specificity. Nowhere did Cook specially threaten to kill or physically harm anyone, as other defendants have. The threat to "take them out," in the context of other language in the posts, could be construed as a wish to remove Cook's nemeses from office. As such, Cook's posts were more a manifesto of grievances than true threats.[12]

---

5 *Cook*, 472 F. Supp. 3d at 328.

6 *Id.* at 330.

7 *Id.*

8 *Id.*

9 *Id.* at 331–32.

10 The others are obscenity, defamation, fraud, incitement, and speech integral to criminal conduct, none of which apply here. *Id.* at 332.

11 *Id.* at 333 (citing Fifth Circuit cases).

12 *Id.* at 335.

The court also held that Cook's posts were protected by the First Amendment because they discussed matters of public concern, given their targets. The court found Cook's posts no more threatening than those of President Trump, who prophesized without consequence that John Bolton would "have bombs dropped on him" following his book's publication. Cook's and Trump's grievances, the court concluded, "are cut from the same cloth," and to prosecute one and not the other would smack of "selective enforcement."[13]

Finally, the court held that criminalizing Cook's posts would impermissibly restrict free speech. As unsavory as they were to their intended targets, they could only be suppressed if doing so was "necessary to serv[e] a compelling state interest."[14] In this case, Cook's First Amendment rights weighed more than the sensibilities of his targets, who only needed to look away to avoid any discomfort.[15]

The court dismissively brushed off the government's reliance on *Conlan* to rebut Cook's facial constitutional challenge of § 2261A(2)(B). Cook was charged with conduct that "caused and would reasonably be expected to cause substantial emotional distress."[16] The 2006 version of the statute required an intent element and a resulting effect on the victim, namely fear of death or serious bodily injury. Under the 2013 version of the statute, and under Cook's charging instrument, "[t]he speaker is guilty, regardless of whether the victim is a reasonable person[, and] whether the victim ever felt actual emotional distress."[17] The court held that its finding that § 2261A(2)(B) was unconstitutional as applied to Cook was enough to dispose of the case, and it dismissed his indictment.[18]

---

[13] *Id*. at 336–37.

[14] *Id*. at 339 (referring to the strict scrutiny test applicable to content-based restrictions on free speech).

[15] *Id*. at 339–40 (invoking *United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000) (persons can protect their own sensibilities simply by averting their eyes)).

[16] *Id.* at 339.

[17] *Conlan*, 786 F.3d at 386; Reply Brief in Response to Government's Response in Opposition to Motion to Dismiss Indictment, *United States v. Cook*, No. 3:30-CR-19, Doc. # 40, 2–3 (N.D. Miss. May 28, 2020).

[18] *Cook*, 472 F. Supp. 3d at 340. The government filed an appeal (Case No. 20-60738 in the Fifth Circuit Court of Appeals).

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.

Hash Values and the Fourth Amendment

By Pierre Grosdidier

The Sixth Circuit Court of Appeals is the latest federal appellate court to consider whether opening a file that has been hash-matched to child pornography constitutes a search under the Fourth Amendment in *United States v. Miller*.[1] The contraband trapping technique at stake is conceptually simple: electronic communication service providers (ESP) filter files that pass through their servers by matching each file's hash value against a database of hash values of known illicit pictures. A hash value is a file's algorithmically-calculated digital fingerprint; it is unique for each file and two files with the same hash value contain the same information.[2] ESPs send trapped files and their originating IP addresses to the National Center for Missing and Exploited Children ("NCMEC"), who then forward the tip to the appropriate police force.[3] Authorities then track down and prosecute the suspect. One of the technique's virtues is that it can be fully automated and does not require ESP employees to review each trapped file because a hash value match guarantees that the file is illicit.[4] The fundamental legal question is whether authorities can open and view the trapped files without first securing a Fourth Amendment search warrant.

In *Miller*, Google trapped two emailed files that it automatically sent to authorities, who viewed them and eventually arrested and prosecuted Miller on child pornography charges. Google did not view Miller's files but had used its own hash algorithm and employees to stock its hash-value database. At some point, therefore, at least one Google employee had viewed the two files and decided they were contraband. Miller appealed his conviction and 150-month prison sentence on Fourth Amendment grounds, *inter alia*.

The court easily rejected Miller's first argument that Google conducted an unreasonable search by filtering his email based on hash values.[5] Google, the court held, is a private entity and not

---

1 *United States v. Miller*, 982 F.3d 412, 2020 WL 7074226, (6th Cir. Dec. 3, 2020).

2 *See generally*, Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 39 (2005). Hash algorithms are not perfect; two different files can have the same hash value, but the odds of a "collision" are "astronomically small." *Id*. The hash value depends on the file's contents, and not on its name. *Id*. n.5.

3 Under 18 U.S.C. § 2258A, ESPs must report known instances of suspected child pornography to the NCMEC's CyberTipline.

4 Unless there is a hash value collision with an innocuous picture (astronomically unlikely), or an error by a Google employee who misjudged erotica (less unlikely).

5 *Miller*, 982 F.3d at 417.

subject to the Fourth Amendment's constraints regarding searches. A private search might give rise to a state tort claim like trespass but does not offend the Constitution. Moreover, none of the three exceptions that arise when a private actor acts as a government agent and that trigger the Fourth Amendment's protection applied here. Google did not perform a public function because it was only protecting its interest when it tracked child pornography, much like stores track shoplifters. Google's file tracking was also not compelled by the government, and Miller identified no nexus between Google and authorities. For these reasons, the court rejected Miller's argument that Google's hash-value tracking violated the Fourth Amendment.[6]

Miller's second argument, that the detective assigned to his case invaded his reasonable expectation of privacy when he viewed the trapped files, fared no better.[7] The court first applied the private search doctrine, which holds that the government does not conduct an illegal search when it is virtually certain that its search does not disclose anything beyond what a prior private search revealed.[8] In *United States v. Jacobsen*, the United States Supreme Court held that no Fourth Amendment violation occurred when DEA agents re-opened a parcel that FedEx employees had previously opened before they called authorities regarding the suspicious white powder it contained.[9] The DEA agents in *Jacobsen* next proceeded to field-test the powder for cocaine. Even though this inquiry exceeded the scope of the FedEx employees' search, the Supreme Court held that it did not violate the Fourth Amendment because it could only affirmatively disclose that the powder was cocaine and not that it was anything else, like "sugar or talcum powder."[10] Such "binary searches", which confirm only the presence of contraband and disclose nothing in the alternative, are not Fourth Amendment searches.[11]

In *Miller*, the court held, opening the files was not a binary search because the detective might have stumbled upon images other than the expected contraband—as unlikely as it was. In that event, the police search would have proceeded beyond Google's and offended the Fourth Amendment. The question, therefore, was whether Google's hash-value matching made it virtually certain that by opening the files, the detective would discover nothing more than what

---

6 *Id.* at 423.

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

8 *Miller*, 982 F.3d at 428 (citing *United States v. Jacobsen*, 466 U.S. 109, 119 (1984).

9 *Id.*

10 *Id.* at 429.

11 *Id.* at 427 (citations omitted). Dogs sniffing luggage for drugs fall under this category. *United States v. Place*, 462 U.S. 696 (1983).

Google had learned when it first viewed the files. Recall that at some point trained Google employees had seen copies of the files and categorized them as child pornography. The issue, therefore, turned on "whether Google's hash-value matching [wa]s sufficiently reliable" to ensure this constitutionally-required virtual certainty, and on the legal test that applied to resolve this question.[12] But, the court saw no need to answer these questions. Miller never challenged the reliability of Google's hashing algorithm below, and the magistrate judge found that the hashing technology was "highly reliable—akin to the reliability of DNA."[13] Because of hashing's generally-accepted reliability and Miller's failure to object, the court held that Google's file matching "satisfie[d] *Jacobsen*'s virtual-certainty test and trigger[ed] its private-search doctrine."[14]

The court also considered adequacy of Miller's defense that the detective's viewing of the files amounted to a Fourth Amendment trespass.[15] In *United States v. Jones*, the U.S. Supreme Court held that attaching a GPS tracking device to a suspect's car qualified as a search because the government committed a physical trespass in its quest for information.[16] In *Miller*, the court analogized the detective's opening of digital files to colonial authorities' intrusion in a person's personal effects and papers, a practice that the Fourth Amendment clearly aimed to curtail. But Miller's trespass defense also failed because of the private search doctrine. Google, not the detective, matched the hash value, which was akin to the act of opening a letter. For these reasons, the court rejected Miller's Fourth Amendment challenge to his conviction.

Miller is mostly consistent with the Fifth Circuit Court of Appeals' *United States v. Reddick* decision.[17] *Reddick* conditionally pleaded guilty to possession of contraband after an ESP's hash filter trapped his illicit smut. As in *Miller*, the court held that Miller lost any expectation of privacy in his files when they were first trapped by a private entity. The *Reddick* court analogized the detective's opening of the files to the DEA agents' chemical test on the suspect powder in *Jacobsen*—an analogy that the *Miller* court expressly rejected because it held that opening the files was not a binary search, for the reason stated above.[18]

---

[12] *Id.* at 429-30.
[13] *Id.* at 430.
[14] *Id.*
[15] *Id.* at 432 (citing *United States v. Jones*, 565 U.S. 400, 405, 406 n.3 (2012).
[16] *Id.* (citing *Jones*, 565 U.S. at 406).
[17] 900 F.3d 636 (5th Cir. 2018).
[18] *Id.* at 639; *Miller*, 982 F.3d at 428-29.

It is important to confine the police search to the trapped files. In *United States v. Ackerman*, the warrantless police search extended to files with hash values that did not match known contraband.[19] The Tenth Circuit Court of Appeals reversed the trial court's denial of Ackerman's motion to suppress for this reason.

Miller, *Reddick*, and *Ackerman* differ in one additional and important detail. In both *Miller* and *Ackerman*, the ESP (Google and AOL, respectively) built their own image databases.[20] These entities could, therefore, claim to have seen the defendants' contraband—a key fact in the applicability of the private search doctrine. The ESP in *Reddick*, Microsoft, relied on a database provided by the NCMEC.[21] Microsoft never viewed the files it sent to the NCMEC, and Reddick could plausibly argue, as he did, that the police's inquiry was more intrusive than Microsoft's.[22] In response, the government argued that based on the detective's "knowledge obtained from the *private searchers*, information in plain view, and his own expertise, he could have concluded with substantial certainty that all of the digital files contained child pornography."[23] But, the Tenth Circuit held in *Ackerman* that NCMEC acted as a government entity for Fourth Amendment purposes. Therefore, it was not quite right to state that the detective obtained his knowledge from *private searchers*.[24] The detective's "virtual certainty" that the files contained contraband originated with NCMEC, a government entity under *Ackerman* that categorized the images as underage pornography. A colorable argument remained, therefore, that the detective in *Reddick* exceeded Microsoft's private search—which never actually looked at the files.

The *Reddick* decision did not directly address this point. It held that "[a] private company determined that the hash values of files uploaded by Mr. Reddick corresponded to the hash values of known child pornography images . . . [,which] qualifies as a 'private search' for Fourth Amendment purposes."[25] It also held that when the detective "opened the files, there was no 'significant expansion of the search that had been conducted previously by a private

---

[19] 831 F.3d 1292, 1306 (10th Cir. 2016) (Gorsuch, J.).

[20] *Miller*, 983 F.3d at 417; *Ackerman*, 831 F.3d at 1294.

[21] Brief of Plaintiff—Appellee, *United States v. Reddick*, No. 17-41116, 2018 WL 1911045, at *5 (5th Cir. Apr. 20, 2018).

[22] Brief of Defendant—Appellant, *United States v. Reddick*, No. 17-41116, 2018 WL 1121804, at **3, 13-14 (5th Cir. Feb. 21, 2018).

[23] Brief of Plaintiff—Appellee, *United States v. Reddick*, 2018 WL 1911045, at **32-33 (internal citations and additions omitted; emphasis added).

[24] *Ackerman*, 831 F.3d at 1297.

[25] *Reddick*, 900 F.3d at 637.

party' sufficient to constitute 'a separate search.'"[26] The decision did not add that the hash values originally came from a government entity, and that without them, Microsoft could not have trapped the contraband because it never actually viewed the files. The question remains, therefore, whether the private search doctrine applies when the private actor identifies contraband based only on hash values supplied by a government entity.

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.

[26] *Id.* at 639.

Robots and Financial Statements: Gaming the System for the Flash Bots

By Ronald Chichester

During the last few years, machine learning engineers have applied increasingly sophisticated natural language processing[1] techniques to reading mundane documents, such as financial reports and annual reports.[2] Other engineers have developed automated methods for writing documents, such as financial reports and financial news items for related websites.[3] We now have the seemingly odd potential for robots writing financial reports that are then read and interpreted by other robots. The rub is that reports tailored for humans are written in one fashion (what we'll call "traditional") and reports tailored for interpretation by robots are written in a different fashion (what we'll called "automated").

There is a segment of investors who are into high frequency trading ("HFT").[4] Recently, HFT investors have created bots that read the sentiment of articles published by financial news organizations, such as Bloomberg. Instead of relying on the factual data in the company's financial report, the bot gauges the sentiment of the author of the article that *refers* to the company's financial report and uses that sentiment to decide whether or not to buy or sell a stock of that company. The idea is that gauging the sentiment in an article leverages the human-interpretation, plus the analysis of the sentiment takes a bot only milliseconds. Swift reaction by the bot can cause the subsequent buy or sell to come before other buy/sell orders

---

1 According to the Wikipedia entry, "Natural language processing (NLP) is a subfield of linguistics, computer science, and artificial intelligence concerned with the interactions between computers and human language, in particular how to program computers to process and analyze large amounts of natural language data. The result is a computer capable of 'understanding' the contents of documents, including the contextual nuances of the language within them. The technology can then accurately extract information and insights contained in the documents as well as categorize and organize the documents themselves" *See* Natural language processing, WIKIPEDIA, https://en.wikipedia.org/wiki/Natural_language_processing (last accessed Feb. 7, 2021).

2 Daulet Nurmanbetov, *Extracting Data from Financial PDFs*, Towards Data Science (Nov. 23, 2019), https://towardsdatascience.com/extracting-data-from-financial-pdfs-dc2fa0b73169.

3 *See, e.g., Natural language processing for financial markets,* Systemic Risk and Systemic Value (June 15, 2019), https://www.sr-sv.com/natural-language-processing-for-financial-markets/.

4 According to the Wikipedia page, "High Frequency Trading (**HFT**) is a type of algorithmic financial trading characterized by high speeds, high turnover rates, and high order-to-trade ratios that leverages high-frequency financial data and electronic trading tools. High-frequency trading, WIKIPEDIA, https://en.wikipedia.org/wiki/High-frequency_trading (last accessed Feb. 7, 2021). For detailed information about this type of trading, *see* MICHAEL LEWIS, FLASH BOYS: A WALL STREET REVOLT (Norton, 2014).

and thus gain an advantage in the market. Unfortunately, as mentioned before, bots are now *writing* these types of articles, and those writing bots do provide a discernible sentiment that other HFT bots can detect. Companies now have the possibility of using the same technology to draft their own articles and tweak the input to skew the sentiment that would be generated by the writing robots employed by the financial press. Essentially, the resulting financial report would be written with a *bot* in mind, rather than a human interpreter, and would also be written in a way that other bots would interpret favorably – without changing the underlying factual information.[5]

There is an obligation under Rule 10b-5 of the Securities and Exchange Act of 1934 not to commit securities fraud by making false statements or omitting relevant information in a way that would deceive an investor.[6] For this short article, the question is: if a company writes a financial statement – via a bot – in a way that causes other *bots* (not human investors) to generate a better sentiment that ultimately affects the market, could that company be liable under Rule 10b-5?

Bots writing specifically for other bots in the hope of affecting the market is a new circumstance. There is little literature on the subject, led alone on-point case law. However, in March 2019, the Supreme Court handed down a decision in *Lorenzo v. SEC*,[7] in which the Court held that those who disseminate false or misleading statements with the intent to defraud—even if they are not the "maker" of the statement—can be found to have violated subsections

---

[5] While little has been written on this topic, there are some basic explanations for the technology involved. *See, e.g.*, Prakhar Ganesh, *High Frequency Trading (HFT) with AI: Simplified*, Towards Data Science (June 19, 2019), https://towardsdatascience.com/high-frequency-trading-hft-with-ai-simplified-a24c00da72e0.

[6] The provisions in Section 10b-5 of the SEC Act include:
§ 240.10b-5 Employment of manipulative and deceptive devices.
It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,
(a) To employ any device, scheme, or artifice to defraud,
(b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or
(c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person,
in connection with the purchase or sale of any security.
(Sec. 10; 48 Stat. 891; 15 U.S.C. 78j)
[13 FR 8183, Dec. 22, 1948, as amended at 16 FR 7928, Aug. 11, 1951].

[7] 139 S. Ct. 1094 (2019).

(a) and (c) of Rule 10b-5 of the federal securities laws, often referred to as the "scheme liability" subsections of Rule 10b-5. Obviously, the Supreme Court did not have bots in mind when it handed down the opinion in *Lorenzo*. However, that ruling potentially forestalls a potential affirmative defense in a 10b-5 suit involving bot-affected circumstances.

For this example, we're going to posit that ACME, Inc. desires to publish a financial statement (such as an annual report) that attempts to forestall a drop in stock price because of mediocre earnings. Knowing that bots often write financial news items, the CEO of the company commissions the IT department to learn how those news-writing bots operate and tailor the company's report such that the review of the annual report by bots provides favorable sentiment, thinking (assuming or hoping) that such sentiment will not prompt a "sell" order by HFT bots that are known to read the other (news-writing) bots. The CEO is adamant that the annual report provide the relevant factual (and factually correct) information. However, the CEO wants the *wording* of the report to be tailored to the news-writing bots, rather than humans. The theory is that humans are smart enough to interpret the information correctly—the bots are not. At this point, the CEO doesn't think that she's gaming the system. For its part, the IT department takes off-the-shelf AI software (for both reading and writing) and develops an experimental system that optimizes the sentiment output based on the factual input. The IT department then (with its AI), drafts the annual report and the company publishes it. As planned, the (third party) bots post not-unfavorable reviews and the stock price of the company remains stable. All is well.

Unfortunately for the company, some human investors actually read the report and surmised what the IT department did. A complaint is then filed with the SEC. The question for the SEC is whether, under *Lorenzo*, did the company intend to defraud investors? Note, it was the news-writing bots under the control of third parties (the financial news organizations) that generated the overly sentimental news items. However, because the company surmised that those financial news organizations used standard AI-writing software, would that have been any different than writing flowery expressions meant to sway human investors? With the proliferation of AI and bots in the financial industry, the question posed in the hypothetical – and similar questions – are likely to be litigated in the near future.

About the Author

Ronald Chichester is a solo attorney who is a past chair of the Business Law Section and a past chair of the Computer & Technology Section of the State Bar of Texas. His area of practice includes computer torts and computer crimes.

Does Facebook have a Duty to Prevent Murder?

By John G. Browning

Of course, the answer to the titular question is "No, they don't"—unless the world in which we live has been magically transformed into the future depicted in the movie *Minority Report*. Yet that didn't prevent the estate of the late Robert Godwin, Sr. from suing Facebook in a case that went all the way to the Ohio Court of Appeals, culminating in an October 2020 opinion.[1] It all began back in 2017, when a man named Steve Stephens murdered Godwin. On the day of the killing, Stephens posted the following to Facebook:[2]

> FB my life for the pass year has really been fucked up!!! lost everything ever had due to gambling at the Cleveland Jack casino and Erie casino . . . I not going to go into details but I'm at my breaking point I'm really on some murder shit . . .FB you have 4 minutes to tell me why I shouldn't be on deathrow!!!! dead serious #teamdeathrow

Godwin's estate sued Facebook based on a common law negligence theory, alleging that the social media platform failed to warn Godwin of Stephens' dangerous propensities of which Facebook should have been aware through its data-mining practices. Bear in mind, Stephens' post was apparently made "minutes" before Godwin's tragic death, and it neither named Godwin or provided any specific murder-related plans. Not surprisingly, the trial court granted Facebook's motion to dismiss.

The estate appealed. In affirming the trial court's dismissal, the Ohio Court of Appeals rejected the notion that Facebook has a special relationship with or owes an abstract duty to everyone in the world. It distinguished the facts in the case from those in which vendors or service professionals (such as doctors or psychiatrists) might have legal duties to prevent a client or patient from committing harm to third parties. Interestingly, the court expressly declined to apply Section 230 of the Communications Decency Act, to this case.[3]

---

1 *Godwin v. Facebook, Inc.*, 160 N.E.3d 372 (Ohio App. Oct. 8, 2020).

2 *Id.* at 376.

3 *Id.* at 383 n.3 ("Facebook also asserted immunity as a defense under the Communications Decency Act of 1996, 47 U.S.C. 230. In light of our conclusion that Godwin has failed to state a claim for relief under Ohio law, we need not resolve the question.").

More troubling is the concurrence written by one judge, who did not "see Facebook's issue"[4] and felt the platform would have a duty because negligence is "in the air."[5] She argued that "public safety should be of primary concern," that Facebook "had information of a potential crime," and that "Only when legal and moral duty converge can courts hear a call for movement and reform."[6] Seriously? Even if Facebook owed a duty to serve as the "pre cogs" in *Minority Report*, the best data-mining in the world won't help where a vague threat is posted minutes before some lunatic chooses a victim at random. This judge's distorted and unfounded view echoes those of legislators around the world seeking to impose broad duties of care on internet services, such as the proposed Online Harms bill in the UK, or the various "Section 230 repeal" bills that would impose duties on social media platforms to notify authorities about "suspicious transmissions." If in fact efforts at repealing Section 230 are successful, we may expect to see left-field opinions akin to the concurrence in this case in the not-too-distant future.

About the Author

John G. 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.

4 *Id.* at 388 (Blackmon, J., concurring).

5 *Id.* at 387.

6 *Id.* at 388.

Will Texas be Primed for Liability of E-Commerce Platforms?

By John G. Browning

In March 2020, my *Circuits* article "Primed for Liability?" looked at the trends among state supreme courts and federal appellate courts in examining whether e-commerce platforms like Amazon should face exposure for strict product liability over allegedly defective products manufactured and sold by third party vendors. Most courts that have considered whether Amazon qualifies as a "seller" have ruled in the online giant's favor, with decisions turning on state laws in Tennessee, Maryland, New York, New Jersey, Arizona, and Ohio. The Sixth Circuit ruled in Amazon's favor in 2019's *Fox v. Amazon*,[1] as did the Ninth Circuit in *State Farm v. Amazon*[2] just months ago. In the June 2020 case of *Oberdorf v. Amazon*,[3] the Third Circuit certified the question of Amazon's potential strict liability to the Pennsylvania Supreme Court. Later in 2020, a California appellate court held that Amazon was strictly liable for the marketplace sale of an exploding battery in *Bolger v. Amazon*.[4] Amidst all of these nationwide developments, my article posited the question: how would Texas rule?

Well, we will soon find out. On December 18, 2020, a panel from the U.S. Court of Appeals for the Fifth Circuit considered the case *McMillan v. Amazon*,[5] a Texas tort case with, as Judge Don Willett recognized, "potentially sweeping implications."[6] In the *McMillan* case, the McMillans purchased a remote control on Amazon.com from a seller in China, "USA Shopping 7693." The McMillans' 19 month-old daughter swallowed the remote control's battery; it was surgically removed, but the lawsuit alleged personal injuries resulting from the battery's caustic fluid. The McMillans sued Amazon in Texas federal district court, alleging strict product liability. Amazon moved for summary judgment, arguing that it was not the remote control's "seller." The district court denied summary judgment, ruling that Amazon was a "seller" under the Texas Products Liability Act because it was "an integral component in the chain of distribution" by enabling the sale.[7] But, agreeing that there was "substantial ground for difference of

---

1 930 F.3d 415 (6th Cir. 2019).
2 2020 LEXIS 36048 (9th Cir. Oct. 20, 2020).
3 818 Fed. Appx. 138 (3rd Cir. Jun. 2, 2020).
4 53 Cal. App. 5th 431 (Aug. 13, 2020).
5 983 F.3d 194, 2020 U.S. App. LEXIS 39847 (5th Cir. Dec. 18, 2020).
6 *Id.* at *1.
7 *Id.* at *7.

opinion" on the scope of "seller" liability under Texas product liability law, the parties jointly moved for an immediate appeal on the "controlling question of law."[8]

The Fifth Circuit, in examining this narrow question of whether Amazon is a "seller" for the purposes of Texas tort law, acknowledged that no Texas court has yet decided this issue. Without available precedent to assist in making an *Erie* guess as to what the Texas Supreme Court would decide, and noting that the difference in state laws and facts made the cases from other circuits "unhelpful," the Fifth Circuit elected to certify the question to the Supreme Court of Texas.[9] Much like the Third Circuit in *Oberdorf*, the Fifth Circuit has decided to let "state-court handiwork supplant federal-court guesswork."[10] And so, the Fifth Circuit certified the following question:[11]

> Under Texas products liability law, is Amazon a "seller" of third-party products sold on Amazon's website when Amazon does not hold title to the product but controls the process of the transaction and delivery through Amazon's Fulfillment by Amazon program?

Oral argument has already been set before the Texas Supreme Court, and many legal observers expect a decision by June. The Court won't get as much guidance from other jurisdictions as originally anticipated: the *Oberdorf* case settled before the Pennsylvania Supreme Court answered its certified question; the California Supreme Court denied review of the *Bolger* case; and the losing side in the Ninth Circuit case has petitioned for en banc rehearing, asking that court to certify the seller question to the Arizona Supreme Court. How will the Court ultimately rule? Amazon has argued that it is more like an auctioneer or a delivery service, merely facilitating online sales for third party products. It points to the Texas Supreme Court's 2008 decision in *New Texas Auto Auction Services, L.P. v. Gomez de Hernandez*, in which the Court held that for strict liability purposes, "sellers" are "those whose business is selling, not everyone who makes an occasional sale" of a product.[12] However, others point out that Texas product liability law doesn't require a "sale" at all; merely "introducing the product into channels of commerce is enough."[13]

---

8 *Id.*

9 *Id.* at *14.

10 *Id.* at *16.

11 *Id.* at *18.

12 249 S.W.3d 402, 405 (Tex. 2008).

13 *Firestone Steel Prods. v. Barajas*, 927 S.W.2d 608, 613 (Tex. 1996).

While we cannot predict how the Court will ultimately rule, it is guaranteed to have important implications for the world of e-commerce and indeed the global economy itself. We will keep you posted.

About the Author

John G. 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.

Privacy Update: What is the Status of the Privacy Law Specialty in Texas?

By Elizabeth C. Rogers

Like many announcements in 2020, the Texas Board of Legal Specialization's (TBLS) accreditation of the International Association of Privacy Professionals' (IAPP[1]) Privacy Law Specialist Certification occurred without much fanfare. Yet, on March 6, 2020, Texas became only one of 3 states in the US, following Minnesota and Alabama, to recognize this certification since the American Bar Association (ABA) accredited the IAPP's certification in 2018.[2]

There are a number of questions that may cross your mind, such as what does it mean to be a Privacy Law Specialist? Should I become a certified Privacy Law Specialist and how? And, last, how do I maintain this specialty? The purpose of this article is to answer these logical questions with practical answers and to offer some insider suggestions from some of us who have already been through the process.

A. What is the Privacy Law Specialist (PLS)?

What distinguishes the PLS from the body of other privacy certifications available through the IAPP is that it is recognized by the ABA and intended only for lawyers practicing in the United States. Privacy law is only the 15th specialty accredited by the ABA.

The PLS distinction carries with it an acknowledgment that an attorney has successfully demonstrated knowledge of relevant privacy laws, regulation and technology; a commitment to staying ahead of new developments in the field; and substantial time devoted to practicing law related to safeguarding personal information. U.S. attorneys who meet the IAPP's rigorous specialist designation requirements may be permitted under their state's rules of professional responsibility to advertise their specialization in privacy law.

In order to apply, attorneys must meet the following requirements:

- Must be admitted in good standing in at least one U.S. state bar;
- Must hold a CIPP/US, plus either a CIPM or CIPT (Certified Information Privacy Manager or Certified Information Privacy Technologist) designation from the IAPP;

---

[1] The IAPP, the International Association of Privacy Professionals, is a not-for-profit organization founded in 2000 that helps define, promote and improve the privacy profession globally.

[2] The TBLS's website announcement of its accreditation of the IAPP's Privacy Law Specialty has been delayed because of interruptions in the ordinary course of business that have arisen during the quarantine.

- Must pass the PLS Ethics Exam administered by the IAPP or submit a recent MPRE score of 80+;
- Must provide proof of "ongoing and substantial" involvement practicing privacy law (at least 25 percent of full-time practice over the last three years);
- Must supply evidence of at least 36 hours of continuing education in privacy law for the three-year period preceding the application; and finally,
- Must provide a personal statement and at least five peer references from attorneys, clients or judges attesting to the individual's privacy law experience.

Though the ABA has requirements of its own in order to approve the PLS specialty certification, largely based on traditional CLE (continuing legal education) requirements, the IAPP still maintains high subjective standards before assigning the PLS certification to any of its members. According to Doug Forman, Director of the IAPP's Certification Programs, "Our review board takes a close look at the personal statement and peer reviews, and there is still an opportunity for the reviewers to say, 'No, this individual has not quite demonstrated a depth and breadth in privacy necessary to warrant the PLS distinction.'"

B. What does the TBLS's accreditation of the IAPP's PLS mean for me?

Because the TBLS has accredited the IAPP's PLS, Texas attorneys who have achieved the certification are now allowed to advertise it. According to the State Bar of Texas Advertising Review Committee[3], there have been some changes in the review process, which have resulted in more convenient reference to specialties in advertising and solicitation material. Specifically:

- The first time that a law specialty is referenced in either an advertisement or biography included within a solicitation communication, the attorney needs to use the full disclosure, e.g., Board Certified in Privacy Law by the International Association of Privacy Professionals.
- For each subsequent reference, in the same advertisement or solicitation communication, the attorney does not need to reference the full disclosure. For example, the reference can be an abbreviated reference such as Certified Privacy Law Specialist, or Board Certified Privacy Law Specialist.
- Abbreviated references to specialties are only allowed when there are multiple references in the same advertisement or biography, and only after the first full disclosure.

---

[3] For specific questions related to advertising or solicitation materials, please consult the Advertising Review Committee of the State Bar of Texas (adreview@texasbar.com or 800-566-4616).

C. How do I prepare for and maintain the certification?

The IAPP provides training for all three certification exams throughout the year[4]. On a quarterly basis, the IAPP will also announce when the next period of review will be for the Privacy Law Specialty. As of the date this issue of *Circuits* is going to press, the next submission period to become an ABA accredited PLS is March 31, 2021.[5]

Following satisfaction of all of the requirements for attaining the PLS certification, successful candidates will need to maintain the certification by receiving 20 credits every two years, after achieving certification, for Continuing Professional Education (CPE)[6]. There are a number of courses available on-line through the national IAPP and sometimes through the local chapters of the IAPP, commonly known as KnowledgeNets. Additionally, members of the Council of the Computer and Technology Section (CTS) are currently working with IAPP stakeholders to become a formal training partner so that CTS members are able to receive CPE credits at the same time that they receive CLE credits for the courses presented by the CTS. Stay tuned!

Texas privacy law attorneys who would like to stand out can do so by attaining the ABA accredited PLS certification that is administered by the IAPP. The process is not inexpensive—the cost of the courses and books add up—but there is only a one-time cost for the certification exams. However, because the passage of federal and state privacy compliance laws is expected only to grow, it may well be worth the investment to not only be distinguished among other practicing privacy attorneys, but also among the non-attorney population of privacy professionals.

---

4 *See* Train, IAPP, www.iapp.org/train/ for a list of available courses and examination details.

5 *See* Privacy Law Specialist, IAPP, www.iapp.org/pls/ for greater details of requirements.

6 *See* IAPP Certification, IAPP, www.iapp.org/certify/cpe/ for details that explain the formal CPE maintenance process.

About the Author

Elizabeth C. Rogers is an integral member of Michael Best's Privacy & Cybersecurity team. Her extensive experience with a variety of regulatory, cybersecurity compliance, and technology-specific privacy matters from her roles as Partner, Chief Privacy Officer, and General Counsel, provides clients with privacy and cyber risk mitigation steps that achieve business objectives.

Elizabeth focuses on issues including breach responses, privacy risk assessments, and enterprise-wide cybersecurity compliance frameworks across industries such as retail, health care, financial services, retail electric providers, education, and state and local governments. She devotes a significant portion of her practice to the energy sector to assist the firm's clients in the utility industry with their unique cybersecurity concerns.

Outside of her law practice, Elizabeth teaches cybersecurity and privacy law topics for the University of Texas School of Information's Master's Program in Identity Management and Security. She is a thought leader on privacy and cybersecurity matters facing businesses, and frequently speaks and is published on emerging trends in these areas.

How to Take Down Fake Websites

By Richard Beem

The situation: You or your client or customer have a business website. A scammer copies it. They use your images. Your text. Pictures and names of your people. Similar but not identical email addresses and phone numbers—they want to redirect your clients or customers into their lair. Their fraudulent site looks just like your real site. They're stealing your identity to commit crimes against you and your clients or customers. Indeed, their crime often starts with website "spoofing," and it usually involves a spoofed URL—similar to your real URL. Their goal is to commit financial fraud and/or to obtain valuable confidential information such as social security numbers, credit card numbers, or medical records with personal identifying information.

Many businesses, including healthcare providers, insurers, and law firms—and their clients and customers—are victims of fake websites, which in turn can enable phishing attacks and data breaches. Information contained in a healthcare record can be worth hundreds of dollars on the black market—as much as ten to forty times the value of a credit card number. A credit card typically can be misused for only a limited amount of time before the fraud is detected and stopped, but personal identifying information, such as social security number and birthdate, can be used to commit all kinds of fraud, such as misdirected tax refunds or unemployment benefits, for extended periods of time.

Law firms, including some of the largest and most sophisticated law firms in the world, are targets of fake websites. The scammers want to intercept confidential information about financial accounts or deals, medical records, or personal identifying information for fraudulent purposes, either to commit fraud directly or to sell the confidential information to others.

The need to act: Now, what are you going to do about the fake website? You must act quickly! Some fake websites are operated for only a few hours—creating immediate havoc with long term consequences—before the scammer moves on to the next target. More than one million fake websites are created *every month*, causing billions of dollars in losses every year. You must act immediately to protect your business and your clients or customers.

This article is directed to spoofing scams—fake websites—in which the scammer spoofs the identity of you or your client or customer to commit financial fraud or to steal confidential information of value. Your first goal should be stop the fraud and its effects as quickly as possible. That's what this article is about: stopping the effectiveness of—and shutting down—

the fake website, and often obtaining transfer of the domain name to the rightful owner—you or your client or customer, as the case may be.

Fake Website Takedowns Distinguished from Other Kinds of Domain Name Disputes and Remedies

There are other kinds of domain name disputes that don't go quite as far as stealing your identity and copying your website. For example, a competitor or knock-off artist or other opportunist might use your trademark or a confusingly similar mark to drive traffic to their "original" website to make sales based on the goodwill associated with your mark.

There also are other kinds of *remedies*, for example, if you want to recover *damages*, perhaps with the initial step of freezing accounts, you might be looking at filing a complaint in federal court, pleading causes of action including Lanham Act violations, and seeking expedited relief, such as a seizure order, without notice, i.e., ex parte.

Best Practices in Trademark Protection and Policing

There are some good steps to take to clear and protect the trademarks and copyrights of you and your clients and customers. Beyond clearance and protection, there is the need to police the marketplace and the web, and to take action against scammers and infringers. These programs take time and forethought to set up and diligence to maintain.

In essence, though it can be broken down further, here are basic steps for trademark and copyright protection and enforcement:

- Clear and register your trademark; and
- Commission a watch service for USPTO trademark activity and for domain name activity; and
- Consider obtaining and maintaining insurance coverage, including cyber insurance.

For purposes of this article, we will assume that you or your clients or customers have legal rights in trademarks or copyrighted works and that you have discovered a fake website—a knockoff of your own site—that seems to be infringing your trademark and/or copyright. The rest of this article will focus on steps to take immediately, but bear in mind that there may be a need to return to and bolster a longer-term program to protect and monitor trademarks and domain names.

Take Down the Cybercriminals

In dealing with scammers, one must know the moves—the attacks and the counters—and one must execute swiftly and surely.

These scams and spoofs are not games. The scammers are committing big-time *fraud*, which is both a crime and a tort. Many of these rackets are run outside American borders, under aliases, and it's hard to find the scammers, let alone apprehend and prosecute them. Nor will you want to wait for a final judgment to be rendered in the ordinary course of civil litigation.

According to the U.S. Department of Justice, losses to the global economy from all forms of cybercrime are measured in the millions of dollars *per minute*—in the trillions per year—and they're still increasing rapidly.

The FBI receives complaints. That might be how you learn of the fake website. They might alert you, but they might not tell you much, and they won't take the steps outlined in this article.

If an FBI investigation is not already underway, you should file a complaint with the FBI—it can't hurt—but, as stated, don't rely on the Bureau to prevent or take down the fake website. They have their hands full with scores of most-wanted cybercriminals, and there must be a thousand times as many active scammers whose frauds have not yet earned them a place on the most-wanted list.

For purposes of this article, we're concerned mainly with minimizing losses to you, your business, and your customers. *You* will need to take the initiative to *stop* any current Internet fraud and to *prevent* it from occurring or reoccurring.

3 Steps for Cybercriminals to Spoof Your Website

In a flash, scammers typically make a few small yet significant changes to *your* content:

- They register a domain name, adopting a spoofed URL, that may differ only slightly from yours;
- They copy your code—names, images and all—and make slight changes to phone numbers and email addresses; and
- As impostors, they start to present themselves as you on the internet and in emails.

Now, web and email traffic, inquiries, confidential information, and orders *intended for you* are diverted to the scammers.

4 Reasons Scammers Copy Your Website

Internet scammers, including those who present fake websites, can have any number of nefarious motives. They might be:

- Holding you up to pay them to transfer the fake domain name to you;
- Siphoning sales from you and delivering fake merchandise to your customers;
- Phishing for confidential information like social security numbers, account numbers, passwords, or medical records for their own illegal use or sale anywhere, such as on the "dark web"; and/or
- Committing financial crimes—stealing money from you and your customers.

One thing you can be sure of: The scammers are up to no good. And *their* fraud committed in *your* name is bad for your business.

Your Company's Website could be Spoofed

You think it couldn't happen to you? Think again. It costs about $10 to purchase a domain name from a registrar, and it takes only seconds to copy a website's code. Stolen images and fake websites abound. Top fashion brands are popular targets. We handle such cases in federal court. But even lower profile businesses—perhaps your company is in this category—can be unsuspecting, making easier targets.

Big tech firms like Facebook, Apple, and Google, and financial companies like Chase and Wells Fargo, are targets of fake website scammers. So are luxury brands like Tiffany and Ray-Ban.

Some of the most sophisticated M&A law firms in New York, and their corporate clients, have been victimized by fake website scammers. The ABA Journal suggests that the scammers were sniffing for M&A deal information. Perhaps they were seeking to reap illegal profits in the stock market based on inside information.

Smaller businesses and law firms also are targets.

Ultimately, if you have any kind of successful business, you are a target for a fake website scammer.

We have dealt with fake website frauds—nipped them in the bud—on behalf of our clients.

Steps to Take Against a Scammer who Copies Your Website:

In short, a lawyer with specific experience in handling trademarks, copyrights, and domain name disputes can act quickly to take the following key steps on behalf of you or your client or customer.

1. Quickly gather and assess the facts. See if you can identify the scammers behind the fake domain name. Unfortunately, the scammers are probably hiding their true identity, which they are permitted to do, for the sake of "privacy." Next best: Identify the registrar of the fake domain name and the host of the fake website servers. This involves use of a WHOIS lookup, which is "not at all intuitive," as admitted by Internet Corporation for Assigned Names and Numbers (ICANN), the organization responsible for managing the Domain Name System (DNS).

2. Create a record of the fraud. File a complaint with the FBI and your local police department. As with most internet content, a simple click by the scammer can make the fake website and all of its contents disappear with little or practically no trace. A record of the fraud will become useful.

3. Investigate insurance coverage and, if potentially applicable, notify the insurer.

4. Prepare and send a Digital Millennium Copyright Act (DMCA) notice and takedown request to the host of the fraudulent website, especially if they're in the U.S. Here again, the scammers are probably devious enough to use a host located outside the U.S., i.e., beyond the reach of the DMCA, which is a U.S. statute.

5. Send a request to Google informing them of the copyright infringement and asking that they remove the scammer from their search results. This might take a few days or more—they receive *over a million* DMCA takedown requests *every day*. Needless to say, the first thing Google looks for is a *complete* DMCA request, including proof that you are the copyright owner. Don't give the scammers precious time to steal from your business or your customers.

6. If you have a trademark, you can prepare and file a complaint under the Uniform Domain-Name Dispute-Resolution Policy (UDRP) with ICANN. A complainant in a UDRP proceeding must establish likelihood of confusion between the fake domain name and your trademark and that the domain name is being used in bad faith. (If you haven't registered your trademark, you should do so.) Successful claimants in a UDRP action

can have the fake domain name transferred to them, so they can shut it down and prevent further fraudulent use.

7. These steps probably will suffice to shut down the particular fake website—the specific URL— and, depending on the situation, maybe that's all you need. But they won't necessarily stop the scammer from popping up with another URL, and they won't recover damages or legal expenses. For that kind of relief, we can file a complaint in federal court to obtain a restraining order and freeze accounts.

8. Take action to prevent or deter future scams. Watch for trademark filings and domain name registrations. We set up these kinds of watches for our clients. Monitor activity on social media. Consider using Google Alerts to identify references to your company and your brands, including competitive or fraudulent activity.

Conclusion

In sum, act quickly to shut the fake website down and have the domain name transferred to the rightful owner, i.e., you or your client or customer. Nip the fraud in the bud.

About the Author

Richard Beem is an active member of the Bar in Texas and Illinois. He practices in the field of patents, trademarks, domain names, and related litigation. Beem earned his J.D. from the University of Houston Law Center, where he was an editor of the Law Review. He clerked for the Hon. Edward S. Smith of the U.S. Court of Appeals for the Federal Circuit before commencing the practice of law based in Chicago. Beem enjoys collaborating with Texas lawyers.

Lawyer's Oath

By Judge Xavier Roriguez

I have formally taken an oath to uphold the United States Constitution on five different occasions. First, when I joined the Army ROTC program at the Massachusetts Institute of Technology in 1979. Again, when I was commissioned as a second lieutenant in 1983. I again took the oath when I became a lawyer in 1987 and I renewed that pledge again when I was administered judicial oaths in 2001 as a Justice on the Texas Supreme Court and in 2003 as a United States District Judge.

Each time I took the oath, it left a different imprint on me. When I was in officer training at Ft. Bragg, NC, the training officer interrupted our session when he was handed a note and then proceeded to inform us that the Soviet Union had amassed a body of troops at the West German border and that we all had been mobilized into active service. Trucks rolled in and we were told to board them for transport to our barracks and deployment. We began boarding the trucks but were soon told to stop and return to our training area. It was a ruse. The training officer then proceeded to inform us what we were doing was important, had a real-world purpose, and we had to be prepared to defend that oath each of us had taken.

When I took the oath to become an attorney, I was more conscious that I would be representing clients and my acts or inactions could materially affect their positions. My appreciation of the rule of law was more limited to an understanding of rules of procedure.

On becoming a judicial officer, the oath took on a greater meaning. I swore "that I will administer justice without respect to persons, and do equal right to the poor and to the rich, and that I will faithfully and impartially discharge and perform all the duties incumbent upon me … under the Constitution and laws of the United States."

As I watched the tragic defilement of the United States Capitol on January 6, I was reminded of the many times I have taken this oath, the times I have administered an oath to newly licensed attorneys, and the thousands I have sworn in to become new American citizens.

As attorneys, we need to reflect on how we got to this awful point in time. Judge Roy Ferguson of the 394th District Court in Texas recently held a virtual ceremony where attorneys were able to renew their vows to uphold the Constitution and rule of law. I applaud him on this initiative.

As lawyers, we represent parties with opposing positions. We do not make up the underlying facts, we do not misrepresent facts to the court, and we do not work in an alternative reality.

As citizens, we need to appreciate that the rule of law—the principle that all people and institutions are subject to and accountable to law that is fairly applied and enforced—can only be maintained when facts, not speculation or conjecture or wishful thinking, are objectively presented.

No matter who we are or who we represent, the rule of law affects us all. It is the foundation for communities of justice, economic and social opportunity, accountable government, and respect for fundamental rights.

I urge you to renew your oath today. I have added one slight modification to the formal oath below. Statements and publications made by attorneys outside the courthouse, whether made in public or private gatherings, in the media or posted in social media, which contain falsehoods, misrepresentations or deceit must be condemned. Each of us must appreciate that what we say and do has consequences.

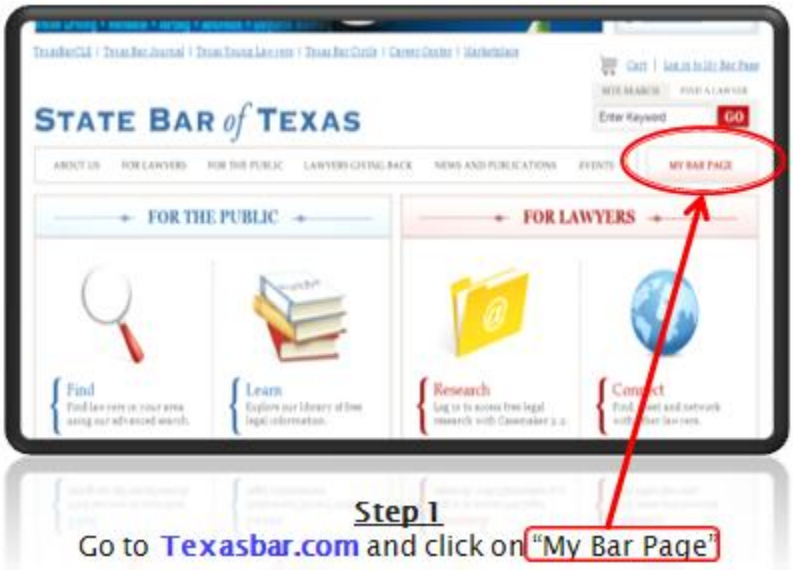
> "I do solemnly swear that I will support the Constitutions of the United States, and of this state; that I will honestly demean myself in the practice of law; that I will discharge my duties to my clients to the best of my ability; and that I will conduct myself with integrity and civility in dealing and communicating with the court and all parties **[and all statements and publications I make]**. So help me God."

About the Author

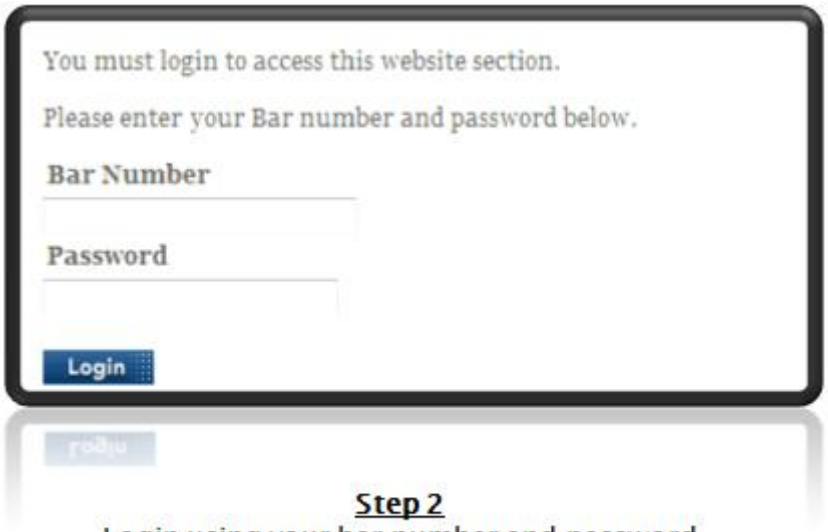
Judge Xavier Rodriguez serves as a United States District Judge in the Western District of Texas and is a Council Member of the Computer and Technology Section.

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

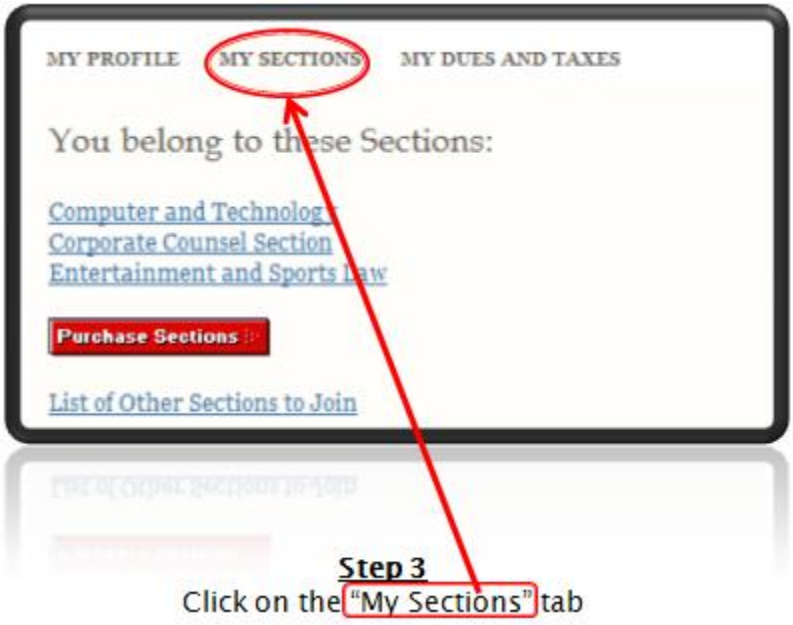
Joining the State Bar of Texas Computer & Technology Section is easy. You can join online by visiting the State Bar of Texas Website at www.Texasbar.com. Please follow these instructions to join the Computer & Technology Section online.



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