COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas
July 2020

Table of Contents

Featured Articles

Short Circuits

CircuitBoards

Table of Contents

Feature Articles:-

Short Circuits:-

CircuitBoards:-

Letter from the Chair

By John G. Browning

As I write this, my last column as Chair of the Computer & Technology Section, I cannot help but pause and reflect on the extraordinary and challenging times in which we find ourselves. These are times that remind us how critical our Section's mission is—educating and assisting Texas lawyers on the importance of technology for practicing law in the 21st century, as well as raising awareness of the risks to data security and privacy. In early May, the website and case management systems for Texas' highest civil and criminal courts were temporarily taken down by a ransomware attack. To ensure continued access to the courts, the Office of Court Administration turned to other technologies, issuing rulings via Twitter and social media.

All of this transpired during a time in which the COVID-19 pandemic has forced lawyers and judges to rely on technology more than ever. Working remotely has made us all keenly aware of both the benefits and risks of technology for our respective practices. With the aid of video conferencing platforms like Zoom, Texas courts have held thousands of hearings since the pandemic began. Lawyers have similarly embraced Zoom depositions and client conferences and made use of remote notarization in order to continue representing our clients' interests. Last month, a Texas court conducted the nation's first Zoom jury trial in Collin County with the aid of one of our Council members, Judge Emily Miskel. Despite a few hiccups, like an occasional camera issue and one juror walking off to take a call, the one-day summary jury trial over an insurance claim was a historic success. At the same time that it offered hope for a possible path forward until life returns to normal, however, the experience also raises legitimate and thorny questions about security, fulfilling a party's right to a fair trial, and the limitations of "virtual deliberations" as jurors try to hash out justice not in the confines of a jury room, but participating remotely from the comfort—and distractions—of their homes.

My own experience has been fairly typical. Client meetings that were once held in person are being conducted via such platforms as Zoom, WebEx, Bluejeans, or Microsoft Teams. Bar committee meetings on Zoom have become routine. A normal week features multiple Zoom depositions and hearings. Last week, I tried a three-day commercial arbitration case via Zoom, hunkered down in a conference room as I delivered my opening statement, examined witnesses, introduced exhibits, and gave closing arguments remotely. Despite an occasional technical glitch here and there that temporarily vexed a lawyer or witness, the proceedings went on the same as if we were all gathered in the same room.

The lives of our clients go on, and so must our lives as their lawyers. CLE is available remotely, and even though our State Bar Annual Meeting is happening remotely instead of in-person, there are still terrific programming options being offered virtually. I'm proud to say that our Section leads the way in providing more CLE programming for the Annual Meeting than any other section, offering timely and valuable instruction on subjects that are incredibly relevant in this "work from home" age. Before I pass the "virtual" torch to incoming Chair Shawn Tuma, I'd like to thank all of our Section members and particularly our Council members for all that they have done and continue to do as ambassadors for our Section. In particular, I'd like to recognize (posthumously) the late Josh Hamilton with our Section's Ralph Brock Lifetime Achievement Award, for his many and varied contributions during a life cut tragically short. I'd also like to recognize both Shawn Tuma and Mark Unger with our Chair's Recognition Awards for 2020: Shawn for his many contributions to raising awareness of cybersecurity issues in society and the legal profession, and Mark for his tireless work in the development, updating, and distribution of our Section's App, which has become a real calling card. Congratulations, Shawn and Mark!

It has been a singular privilege to serve as your Chair this past year. Thank you, one and all.

John G. Browning
2019-2020 Chair
Computer & Technology Section
State Bar of Texas

COMPUTER AND TECHNOLOGY SECTION

Letter from the Editor

By Sanjeev Kumar

Welcome to the fourth and final issue of *Circuits* for the 2019-20 bar year! Our apologies for a somewhat delayed publication of this volume due to some unavoidable circumstances. The pandemic caused by COVID-19 is getting worse across our great state of Texas and the country. Please stay safe and take precautions to avoid unnecessary risk. The Computer and Technology Section has a lot of tools available to help us lawyers remain productive remotely in our practice. The accomplished members of the Computer & Technology Section Council are always willing to help in any way possible during these trying times, so please do not hesitate to contact us through our section administrator at admin@sbot.org.

In our Feature Articles, we start with a contribution from Judge Xavier Rodriguez discussing the admissibility of wrongfully obtained evidence in litigation. Next, our Section Chair, John Browning, in collaboration with guest authors Grant DuBois and Katherine Frisbee, discuss the challenges associated with e-Discovery and use of ephemeral applications and the consequences of intended/unintended spoliation of evidence. These articles are even more relevant due to the changed landscape of business operations brought about due to the COVID-19 related shutdowns and remote operations.

Recent times have seen increased scrutiny of data privacy issues and a number of new laws, such as the GDPR in the European Union and the CCPA in California, have been enacted. The increased use of personal spaces and equipment in business, along with the sharing of health data as a result of COVID-19, may have resulted in some of us to have increased interest in data privacy issues. If you have any interest in attaining certification as a certified information privacy professional, our co-editor, Kristen Knauf, shares her experience and knowledge in the next feature article to help you in achieving your goal.

As a result of the pandemic, there has been an increased interest to have an estate plan in place. Unfortunately, a number of clients are unable or unwilling to have face-to-face meetings for notarizations of their legal documents. To help you tackle the remote notarization of legal documents, guest author, Kirsten Kumar, provides an informative discussion on the various aspects of remote notarization in a very topical article.

Next, our former Section Chair Ron Chichester provides an introductory discussion on how we lawyers can use artificial intelligence (AI) to help us with tasks and make ourselves more efficient. This is a continuation of his articles in the previous issues of *Circuits* regarding AI.

We start our *Short Circuits* section by continuing with the data privacy theme of some of the other feature articles in this issue, in which our past editor and council member, Pierre Grosdidier, sheds some light on aspects of the French Data Protection Act.

In our next article in *Short Circuits*, Ron Chichester discusses the use of public ports for charging our mobile devices and "*Juice Jacking*."

In our *Circuitboards* section, Council Member Alex Shahrestani continues his series of articles to help us automate our practice by providing a tutorial on how to automate social media postings using *HootSuite*.

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

Kind Regards,
Sanjeev Kumar, Editor

Is Wrongfully Obtained Evidence Admissible in Civil Cases?

By Judge Xavier Rodriguez

A. Generally – yes, but only if the litigant and his attorney were not involved in the procurement of the material, and the material is not privileged.

"In civil cases, even illegally obtained evidence may be admissible at trial."[1] In this breach of contract case, relators anonymously received three separate packages of documents that were illegally obtained from real party in interest, BDLI. Relying upon *Sims v. Cosden Oil & Chem. Co.*,[2] the *In Re Strategic Impact Corp*. court restated that "[C]ourts do not concern themselves with the method by which a party to a civil suit secures evidence pertinent and material to the issues involved ... hence evidence which is otherwise admissible may not be excluded because it has been illegally and wrongfully obtained."[3] Mandamus was only conditionally granted in *In Re Strategic Impact Corp*. because the trial court did not conduct an in-camera review of the documents to determine whether any of them were privileged.

In another case, the plaintiff challenged a civil traffic violation fine, arguing he was injured by the use of allegedly illegally obtained evidence to prove the traffic violation. The plaintiff argued that the operator of the traffic recording camera was not appropriately licensed and accordingly the video was taken illegally. The U.S. Fifth Circuit Court of Appeals, interpreting Texas law, concluded that "illegally obtained evidence may be admitted in civil traffic violation proceedings, and therefore the use of such evidence against Appellants creates no injury."[4]

In *Wren v. Towe*,[5] the Wrens filed suit against two law enforcement officers under 42 U.S.C. § 1983 for violations of the Fourth and Fourteenth Amendment protections against the unreasonable seizure of their truck. The Fifth Circuit held that "[e]xclusion of the evidence found by Norris and Towe on the basis that they had no legal right to search the vehicle would, in effect, be an application of the exclusionary rule to this case. Such an application would be

---

1 In Re Strategic Impact Corp., 214 S.W.3d 484, 488 (Tex. App.-Hou. [14th Dist.] 2006, orig. proc.).
2 Sims v. Cosden Oil & Chem. Co., 663 S.W.2d 70, 73 (Tex. App.--Eastland 1983, writ ref'd n.r.e.).
3 In Re Strategic Impact Corp., 214 S.W.3d at 488.
4 Bell v. Redflex Traffic Sys., Inc., 374 F. App'x 518, 520 (5th Cir. 2010).
5 Wren v. Towe, 130 F.3d 1154, 1157 (5th Cir. 1997).

inappropriate. The Supreme Court has never applied the exclusionary rule to civil cases, state or federal."[6]

B. What about statements secured in violation of Miranda? Generally, the exclusionary rule only applies to criminal cases or quasi-criminal cases.

Statements obtained in violation of an individual's *Miranda* rights, however, have been treated differently. Some cases limit, generally, the applicability of the exclusionary rule to civil actions for forfeiture or to cases characterized as "quasi-criminal."[7] Absent participation by the private party proffering any such statements in the civil case, a number of jurisdictions, including Texas, hold that the exclusionary rule, which requires that illegally obtained evidence cannot be used in a criminal proceeding against the victim of an unlawful search and seizure, does not apply to civil proceedings.[8]

C. In a civil proceeding, can the Government use evidence obtained wrongfully in a criminal case? Yes, assuming the same governmental entity pursuing the civil case was not involved in the procurement of the evidence.

In *United States v. Janis*,[9] Los Angeles police officers searched the defendant's apartment for bookmaking paraphernalia. The officers seized cash and wagering records and arrested the defendant. The police officers then notified the Internal Revenue Service that the defendant had been arrested for bookmaking activities. After ascertaining that the defendant had not filed wagering tax returns for his bookmaking enterprise, the IRS assessed back wagering taxes against him. The IRS based the assessment exclusively upon the evidence obtained by the Los Angeles police officers in their search of the defendant's apartment. The Supreme Court recognized that the "seminal cases that apply the exclusionary rule to a civil proceeding involve 'intrasovereign' violations."[10] Absent any proof of federal participation in the illegality, the Supreme Court found no issue with the use of the records in the civil case.

D. Wiretap violations have produced mixed results.

Any "person" whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of 18 U.S.C. § 2511 may bring a civil action under 18 U.S.C. § 2520 for damages. A person may bring suit only for the unlawful interception, disclosure, or use of his or her own

---

6 *Id.* at 1158.

7 *See, e.g.*, C.W. v. Zirus, No. SA-10-CV-1044-XR, 2012 WL 3834904, at *2 (W.D. Tex. Sept. 4, 2012).

8 *Id.*

9 United States v. Janis, 428 U.S. 433 (1976).

10 *Id.* at 456.

communication and has no standing to seek recovery for the unlawful interception, disclosure, or use of another's communication.[11] "Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter."[12]

In a petition to modify the parent-child relationship, one party sought to prevent the admission of tape-recorded telephone conversations and messages left on an answering machine because the recordings allegedly violated state and federal wiretap laws. The court concluded that "Mancini was entitled to consent to the tape recording, both for himself and for L.M.M. as her joint managing conservator."[13]

E. Self-help discovery and False Claims Act/whistleblower cases.

Many employees pursuing qui tam, whistleblower, and other employment-related claims against their employers engage in "self-help discovery," using their access to files and databases to collect and gather, in violation of company policy, documents and data relating to their claims. Some courts have acquiesced to this behavior as long as the party removing the documents established that such removal was reasonably necessary to pursue the claim and the data was not otherwise disseminated.[14]

---

[11] *See, e.g.*, Janecka v Franklin, 684 F. Supp. 24 (S.D.N.Y. 1987), aff'd, 843 F. 2d 110 (2d Cir. 1988).

[12] 18 U.S.C. § 2515.

[13] Allen v. Mancini, 170 S.W.3d 167, 173 (Tex. App.-Eastland 2005, pet. denied*);* Kotrla v. Kotrla, 718 S.W.2d 853, 855 (Tex. App.-Corpus Christi 1986, writ refused n.r.e.) ("Tape recordings, even if obtained without the consent of a party to it, are admissible if the proper predicate is lain."). *But see* Collins v. Collins, 904 S.W.2d 792, 799 (Tex. App.-Hou. [1st Dist.] 1995, writ denied with per curiam, 923 S.W.2d 569 (Tex. 1996)) ("Although the Texas wiretap statute does not specifically provide for the exclusion of illegally obtained 'communications,' the provisions for a cause of action for divulging wiretap information and the injunctive remedies provided in [Tex. Civ. Prac. & Rem. Code] section 123.004 are sufficient to rebut the presumption of admissibility under rule 402. Because the tapes were illegally obtained under the federal and state statutes, the trial court should not have admitted them into evidence on the issue of custody.").

[14] *See* Cafasso v. General Dynamics C4 Sys., Inc., 637 F.3d 1047, 1062 (9th Cir. 2011) (noting "some merit" in a public policy exception to disclosure of confidential information by relators in furtherance of FCA actions, but declining to apply such exception); *see also* Erhart v. Bofi Holding, Inc., No. 15-CV-02287-BAS-NLS, 2017 WL 588390 (S.D. Cal. Feb. 14, 2017) (plaintiff did not breach the confidentiality agreement due to a public policy exception and the documents taken were carefully

F. Using evidence wrongfully obtained, however, may result in discovery sanctions being assessed.

In a real estate dispute, one party trespassed upon the land to make an appraisal. Plaintiffs objected to the entirety of the appraiser's testimony for failure to follow former Tex. R. Civ. P. 166(b) (now Rule 196.7 - Request or Motion for Entry Upon Property). The trial court excluded the testimony as a discovery sanction and the court of appeals affirmed.[15]

In *Xyngular Corp. v. Schenkel*,[16] the Xyngular parties alleged that (1) Schenkel wrongfully encouraged an employee to steal documents belonging to Xyngular, (2) Schenkel knowingly received and reviewed those stolen documents, (3) Schenkel then shared those stolen documents with his litigation counsel, (4) Schenkel failed to return those stolen documents to their owners, (5) Schenkel used those stolen documents in the litigation, and (6) Schenkel engaged in a course of action to cover up his wrongful conduct. Xyngular also argued that many of the documents Schenkel obtained contain privileged, confidential, and sensitive information. Rejecting Schenkel's claims that he cannot be sanctioned for prelitigation conduct, the court concluded "that it may use its inherent powers to sanction a party who circumvents the discovery process and the rules of engagement employed by the federal courts by improperly obtaining evidence before litigation and then attempting to use that evidence in litigation."[17] The court stated that "[I]t is an improper litigation tactic to use a disgruntled employee to secretly obtain non-public internal business documents from an opposing party. And a court may sanction a party for wrongfully obtaining the property or confidential information of an opposing party."[18]

---

selected and narrowly tailored to support his claims). *But see* JDS Uniphase Corp. v. Jennings, 473 F. Supp. 2d 697, 704 (E.D. Va. 2007) ("California's declared public policy does not invalidate the [proprietary information agreement] or authorize Jennings to pilfer or convert JDSU's documents.").

15 Schenck v. Ebby Halliday Real Estate, Inc., 803 S.W.2d 361, 373 (Tex. App. -Ft. Worth 1990, no writ).

16 Xyngular Corp. v. Schenkel, 200 F. Supp. 3d 1273, 1300 (D. Utah 2016), aff'd sub nom. Xyngular v. Schenkel, 890 F.3d 868 (10th Cir. 2018).

17 *Id.* at 1315.

18 *Id.* at 1316. *See also* Glynn v. EDO Corp., No. JFM-07-01660, 2010 WL 3294347, at *3 (D. Md. Aug. 20, 2010) ("Under its inherent powers, a district court may sanction a party for wrongfully obtaining the property or confidential information of an opposing party."); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 571 (S.D.N.Y. 2008) (judicial "integrity is threatened by admitting evidence wrongfully, if not unlawfully, secured."). The Magistrate Judge recommended that the e-mails wrongfully procured "be precluded from use in the litigation, but not for impeachment purposes should Defendants open the door." *Id.*

G. Ethics Rules.

1. Texas Disciplinary Rules of Professional Conduct 4.04.

"In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person."[19] Outside of conflict disqualification cases, no Texas case was found interpreting this rule in the context of an attorney using wrongfully obtained evidence. In *Sosa v. Union Pac. R.R. Co.*,[20] a truck/train collision case, the train's conductor received two telephone calls from someone who claimed that he worked for Union Pacific's legal team. The caller told the conductor that the train's horn did not sound prior to the collision and asked the conductor if he wanted to change his previous statement about the horn's sounding. The call was traced to a longtime friend of one of the plaintiffs' attorneys. The court addressed the issue of whether the plaintiffs should suffer ultimate sanctions because of the conduct of their lawyers. Violation of Rule 4.04(a) was not an issue in this appellate proceeding.

In addressing the Missouri version of Rule 4.04, in *In re Eisenstein*,[21] the Missouri Supreme Court considered whether an attorney violated Missouri Rule 4-4.4(a) by utilizing payroll information and a list of direct examination questions that were improperly procured by the husband in a divorce case. The attorney admitted that he reviewed the information provided by the husband, realized it was "verboten," and did not immediately disclose his receipt of the information to opposing counsel. The court suspended the attorney for a period of six months.

2. ABA Formal Opinion 11-460 (Aug. 4, 2011).

This opinion addressed a lawyer's ethical duty upon receiving copies of e-mails between a third party and a third party's lawyer. The opinion concludes that the issue is beyond the scope of ABA Rule 4.4(b). However, it recognizes that "courts may require lawyers in litigation to notify the opposing counsel when their clients provide an opposing party's attorney-client confidential communications that were retrieved from a computer or other device owned or possessed by the client." If the court recognizes such a duty, the lawyer may be subject to discipline under Rule 3.4(c) for knowingly failing to notify opposing counsel. Even if there is no

---

[19] Tex. Disciplinary Rules of Prof. Conduct, Rule 4.04(a) (1989).

[20] Sosa v. Union Pac. R.R. Co., No. 13-13-00257-CV, 2015 WL 2353024, at *1 (Tex. App.-Corpus Christi May 14, 2015, no pet.).

[21] In re Eisenstein, 485 S.W.3d 759, 762 (Mo. 2016).

clear notification obligation, it often will be in the lawyer's best interest to give notice and obtain a judicial ruling on admissibility before reviewing the documents.

H. Attorney Disqualification.

In *In re Meador*, the Texas Supreme Court considered whether the interests of justice required disqualification of a lawyer who had received an opponent's privileged materials "outside the normal course of discovery."[22] The court stated that ABA Formal Opinions were an aspirational goal, not a standard for disqualification, and that no specific Texas disciplinary rule applied to the circumstances of this case.[23] The court explained that a lawyer should not be disqualified for a disciplinary violation that has not resulted in actual prejudice to the party seeking disqualification.[24]

> "If a lawyer receives privileged materials because the opponent inadvertently produced them in discovery, the lawyer ordinarily has no duty to notify the opponent or voluntarily return the materials. Rather, the producing party bears the burden of recovering the documents by establishing that the production was involuntary."[25]

In *Meador*, the court expressed "no opinion on the proper standard for disqualifying an attorney who was directly involved in wrongfully procuring an opponent's documents."[26]

I. Criminal laws to consider.

Receiving stolen property, knowing the same to have been taken, stolen, or embezzled may violate 18 U.S.C. § 662.

A client may face criminal charges for unlawfully intercepting emails, but an attorney does not violate the Federal Wiretap Act by producing them in response to discovery requests.[27]

Any person who knowingly mails or transports or ships in interstate or foreign commerce by any means, including by computer, any child pornography; or knowingly receives or distributes

---

[22] In re Meador, 968 S.W.2d 346, 351 (Tex. 1998).
[23] *Id.*
[24] *See also* In re Nitla S.A. de C.V., 92 S.W.3d 419, 422 (Tex. 2002).
[25] In re Meador, 968 S.W.2d at 352.
[26] *Id.*
[27] Epstein v. Epstein, 843 F.3d 1147 (7th Cir. 2016).

any child pornography that has been mailed, or shipped may violate the Child Pornography Prevention Act.[28]

J. Potential civil claims.

Assuming your client signed a contractual agreement not to disclose information, a breach of contract claim could be raised.

If any of the information taken by your client contains trade secrets, a theft of trade secrets claim could be asserted.

K. Conclusion.

Navigating the minefields in this area is tricky. Generally, if an attorney or litigant *receives unsolicited* material that was wrongfully taken, the material may be used in a civil case (provided that the material is not privileged). If the litigant actively *procures* such material (self-help discovery), the litigant could face civil claims of breach of contract, breach of fiduciary duty, IP theft, conversion, etc. If the documents taken were carefully selected and narrowly tailored to support whistleblower claims and not otherwise disseminated, some courts have allowed such self-help discovery and dismissed any counterclaims based on public policy. Some courts, however, are uncomfortable with conduct that takes place outside the scope of formal discovery rules and have issued discovery sanctions. Should counsel come into the possession of privileged or wrongfully obtained data, counsel may wish to consider notifying opposing counsel and obtaining a court ruling on future use to avoid any disqualification attempt, sanctions, or disciplinary proceedings.

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.

[28] 18 U.S.C. § 2252.

Here Today, Gone Today: Ephemeral Messaging Problems in Litigation won't Disappear

By John G. Browning, Grant DuBois and Katherine Frisbee

In its 2020 survey of federal judges, e-discovery company Exterro asked what new type of data lawyers should be most worried about over the next five years. The overwhelming choice, with nearly 70% of the votes, was ephemeral apps like Snapchat, Wickr, Signal, Confide, and the like. While the concept of exchanging written messages that self-destruct is not a new one, rapidly advancing technology has taken it to a new level. These apps allow users to send each other encrypted, private messages that can be set to automatically delete themselves without a trace after a set time period. While convenient for consumers, the litigation and compliance implications for companies both large and small are staggering. And as more companies utilize technology to permit employees to work remotely during the COVID-19 pandemic, these implications take on heightened importance.

I. A BIT OF BACKGROUND

The process of erasing the ephemeral message is complex, and usually depends on the service used. There is a spectrum of ephemeral messaging systems. While some systems delete the messages automatically after the recipient reads the message, others delete the message after a certain length of time or only delete the message when the user manually deletes it.[1] Before the message is erased, the encryption of messages "prevents eavesdroppers from copying a message while it is in transit from the sender to the recipient" and passwords are sometimes used to ensure recipients confirm their identity before accessing the message.[2] When an ephemeral message is erased, every copy of that message is erased on the "machines that a message has based through, including the host servers."[3] It is important to note the difference between the terms "delete" and "erase."[4] When a file is deleted, it is not gone forever; it is just hard to find now.[5] Data recovery software can still find deleted files and recover them.[6] In

---

1 *Top 4 Benefits of Ephemeral Messaging for Security Professionals*, WICKR (Apr. 7, 2020), https://wickr.com/top-4-benefits-of-ephemeral-messaging-for-security-professionals/.

2 *See* Paul Gil, *How Ephemeral or Self-Destructing Messaging Works*, LIFEWIRE (Aug. 9, 2019), https://www.lifewire.com/self-destructing-messaging-4102193.

3 *Id.*

4 Tim Fisher, *Wipe vs Shred vs Delete vs Erase: What's the Difference?*, LIFEWIRE (Mar. 20, 2020), https://www.lifewire.com/wipe-vs-shred-vs-delete-vs-erase-whats-the-difference-2619146.

5 *Id.*

6 *Id.*

contrast, when a file is erased, it is truly gone.[7] There are three ways to erase data: (1) use a program to "wipe" or "scrub" the data; (2) "disrupt the magnetic field of" the object storing the data; or (3) "physically destroy the device."[8] Wiping and scrubbing the data are different in terms of scope—wiping erases *everything* on the device; scrubbing (also known as "shredding") erases just the selected files.[9] This self-erasing technology has brought a new line of challenges to the courts in terms of discovery, evidence, subpoenas, and sanctions—this article will consider discovery and sanctions regarding ephemeral messages.

Beyond the nature of the communications themselves, some of the more perplexing questions about such disappearing messages being used by employees involve the implications for lawsuits. What counts as electronically stored information (ESI) for purposes of discovery and spoliation? If the contents of the messages are irretrievable, how are litigants to know whether Employee A divulged trade secrets to Employee B, or simply discussed weekend plans? Is this information better discovered through depositions, anyway? This is where the judicial "smell test" of Federal Rules of Civil Procedure ("FRCP") 37(e) should be applied.

FRCP 37(e) was adopted in 2015 in an attempt to reduce reliance on state law or inherent authority when it comes to the spoliation of ESI, since electronic data storage and transmittal had grown exponentially since the rule's last amendment in 2006. The spirit of the rule is simply to give courts discretion to cure when there has been a finding that a party opponent has been prejudiced by the loss of ESI, or also when a party opponent has been found to have intentionally acted to deprive another party of the ESI's use in litigation.[10] In either event, the court may order measures to cure the prejudice, up to and including dismissing the action.[11]

II. EPHEMERAL MESSAGING IN LITIGATION, PART ONE: *WAYMO LLC V. UBER TECHS., INC.*

A. Background of the Case

In *Waymo LLV v. Uber Techs. Inc.*, Google's self-driving autonomous vehicle unit, Waymo, sued Uber for "trade secret misappropriation, patent infringement, and unfair competition" regarding its budding self-driving car technology.[12] Evidence indicated that the "former star

---

7 *Id.*

8 *Id.*

9 *Id.*

10 FED. RULE CIV. PRO. § 37(e)(1-2).

11 *Id.* § 37(e)(2)(c).

12 Waymo LLC v. Uber Techs., Inc., No. C 17-00939 WHA, 2017 WL 2123560, at *1 (N.D. Cal. May 15, 2017).

engineer" at Waymo, Anthony Levandowski, "downloaded over 14,000 confidential files immediately before leaving his employment" at Waymo and promptly joining Uber's self-driving technology team as the lead.[13] There was a "total absence of any evidence" that Levandowski "returned or otherwise surrendered" these 14,000 files.[14] Levandowski downloaded 9.7 gigabytes of company data from Waymo onto his personal device using a "portable data transfer device" that was plugged into his laptop for about eight hours.[15] Levandowski proceeded to (1) completely wipe his laptop's data; (2) export even more documents regarding Waymo and its self-driving car technology onto his personal device; and (3) then resign from Waymo without giving notice.[16] There was evidence that before Levandowski resigned, he and Uber had arranged for Uber to acquire Levandowski's new self-driving car company, Otto, for $680 million.[17]

During the contentious discovery process, "the belated discovery of inflammatory communications by a former Uber employee," Richard Jacobs, "came to light outside the normal discovery process."[18] Jacobs stated not only that Uber was on a "'mission' to 'steal trade secrets,'" but also that Uber used "clandestine and concerted efforts to steal competitor's trade secrets."[19] By this, Jacobs was referring to Uber's use of ephemeral messaging. Jacobs viewed himself as a whistleblower within Uber when be made "efforts to expose . . . certain alleged activities," like ephemeral messaging, that he believed "were wrongful, unethical, and/or illegal."[20] Jacobs explained the ephemeral messaging, saying it was among "certain alleged information-gathering activities" that "were hidden from any oversight or legal process by an *elaborate set of technical protections*."[21] Jacobs accused Uber employees of meeting specifically to discuss how to ensure the secrecy of meetings between Uber and Otto.[22] Furthermore, Jacobs claimed that Uber instructed and trained its employees "on how to use 'ephemeral communications'. . . to 'prevent[] Uber's unlawful schemes from seeing the light of

---

13 *Id.*

14 *Id.* at *6.

15 *Id.* at *2.

16 *Id.*

17 *Id.* at *2-3.

18 Waymo LLC v. Uber Techs., Inc., No. 3:17-CV-00939, 2017 WL 6501798, at *1 (N.D. Cal. Dec. 15, 2017).

19 *Id.*

20 *Id.* at *3.

21 *Id.* (emphasis added).

22 *Id.* at *4.

day.'"[23] Specifically, Uber used Wickr and Telegram, ephemeral apps, in these communications. Ultimately, what became known as the "Jacobs Materials" included a "demand letter, resignation email, and settlement agreement"[24] between Jacobs and Uber described as a "jackpot settlement."[25]

B. Regarding Sanctions for Spoliation of Evidence through Ephemeral Messaging

The court described these materials as "a barrage of scandalous allegations against Uber" that included "deliberate spoliation" of evidence.[26] Upon learning about these messages, Waymo wasted no time in arguing that Uber "tossed out evidence and engaged in litigation misconduct."[27] While Judge William Alsup was "not inclined" to hold Uber in contempt during an August 2017 pretrial hearing, the judge said he would consider informing the jury about "Uber's misconduct, if any," though Waymo was ultimately unsuccessful in obtaining a favorable jury instruction.[28]

Waymo also submitted a motion for sanctions for spoliation of evidence.[29] Citing FRCP 37(e), Waymo sought an adverse-inference instruction against Uber based on its allegation that Uber had spoliated evidence.[30] The court held that FRCP 37(e) was the controlling legal standard because the spoliated evidence was electronically stored.[31] The relevant portion of FRCP 37(e) states:

> If electronically stored information that *should have been preserved* in the anticipation or conduct of litigation is lost because a *party failed to take reasonable steps to preserve it*, and it *cannot be restored or replaced through additional discovery*, the court:
>
> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:

---

[23] *Id.* at *6 (quoting ECF No. 2307-2 at 9).

[24] Waymo LLC v. Uber Techs., Inc., No. C 17-00939 WHA, 2018 WL 646701, at *2 (N.D. Cal. Jan. 30, 2018).

[25] *Id.* at *18.

[26] *Id.* at *2.

[27] *Id.* at *1.

[28] *Id.*

[29] *Id.* at *14.

[30] Waymo LLC, 2018 WL 646701, at *14.

[31] *Id.*

(A) presume that the lost information was unfavorable to the party;
(B) instruct the jury that it may or must presume the information was unfavorable to the party; or
(C) dismiss the action or enter a default judgment.[32]

Judge Alsup first analyzed the requirement of anticipated litigation, an objective standard. The question was not whether Uber "in fact reasonably foresaw litigation;" the question was "whether a reasonable party in the same factual circumstances would have reasonably foreseen litigation."[33] The court not only found that a "reasonable party in Uber's circumstances would have reasonably foreseen this litigation," but also that "Uber *actually* foresaw this litigation in January 2016" through its acquisition of Otto because Uber had already "previously insisted as much" when it argued that it had "anticipated, foresaw, and painstakingly planned for this very litigation" [34] and had even hired counsel in anticipation of "super duper litigation."[35] Judge Alsup was not convinced by Uber's "performance deserving of an Academy Award" trying to hastily flip their argument.[36] Therefore, this requirement was satisfied.

Judge Alsup next addressed the spoliation of evidence requirements. Waymo organized the allegedly spoliated evidence that Uber did not "take reasonable steps to preserve" into five categories.[37] One of these categories was the ephemeral messages, described as "hundreds of text messages among Levandowski, Ron, Kalanick, and Qi [that] have been deleted."[38] Uber did not dispute that these ephemeral messages had been lost and could not be "restored or replaced through additional discovery."[39] Instead, the company argued that sanctions would not be appropriate because Waymo's motion was untimely, the ephemeral messages were irrelevant, and because Uber "acted in good faith."[40] The court ultimately found that the motion was timely filed to retain relief, and that Uber's argument that the ephemeral messages were irrelevant was "similarly meritless."[41] Although Uber urged that these messages contained

---

[32] FED. RULES CIV. PROCEDURE § 37(e) (emphasis added).
[33] Waymo LLC, 2018 WL 646701, at *14 (quoting Micron Tech., Inc. v. Rambus Inc., 645 F.3d 1311, 1320 (Fed. Cir. 2011)).
[34] *Id.* at *15.
[35] *Id.* (quoting Dkt. No. 515-14 at 4-5, 50-51).
[36] *Id.*
[37] *Id.* at *16.
[38] *Id.*
[39] Waymo LLC, 2018 WL 646701, at *17.
[40] *Id.*
[41] *Id.*

information about "innocuous business matters," instead of trade secret misappropriation, the court rejected this argument. The ephemeral messages were not only relevant, but "the very heart of this case."[42] This left only the final requirement: bad faith.

As for bad faith, the court acknowledged that while there was considerable evidence of bad intent on Uber's part with the Jacobs materials in mind, at the same time it was worried that Waymo was using the court as a crutch to fill in the gaps of its case with adverse inferences. This was because the court felt Waymo was either "unwilling or unable to prove its case" through its own evidence and witnesses.[43] As a result, the court refrained from levying spoliation sanctions. However, the order still reserved the decision of whether Uber "spoliated evidence with the intent to deprive another party of its use in litigation" for the trial court.[44]

C. Use of Ephemeral Messaging Apps Used in Evidence against Uber

Regarding the ephemeral messages, the court held that Waymo would be "allowed to adduce facts showing this to the jury," but ultimately reserved the decision about giving an adverse-inference instruction.[45] The court also allowed Waymo to "adduce certain facts" at trial to show that Uber was trying to learn more about their self-driving car technology, and that Uber "sought to minimize its 'paper trail'" through its ephemeral messaging.[46] Though Waymo could use the evidence of Uber's ephemeral communication use to explain the gaps in its proof of misappropriation, the court made it clear that the ephemeral messaging would not be permitted "to the extent that it becomes cumulative, invites improper speculation, vilifies Uber without proving much else, or threatens to overwhelm the trial and distract from the merits of the case."[47] Judge Alsup granted Waymo permission to use evidence of Uber's use of ephemeral messaging at trial, but also ruled that Uber would be allowed to present evidence and argument defending its use of ephemeral communications and showing that the use of these apps "shows no wrongdoing, including pointing out Waymo's own use of ephemeral communications."[48] With this said, despite all the contention leading up to trial about the use of ephemeral communications in evidence, the jury heard very little about ephemeral

---

[42] *Id.*
[43] *Id.* at *18.
[44] *Id.*
[45] Waymo LLC, 2018 WL 646701, at *19.
[46] *Id.*
[47] *Id.* at *3.
[48] *Id.* at *21.

messaging in trial, and the case settled four days into trial with Waymo accepting a $245 million investment stake in Uber.[49]

III. EPHEMERAL MESSAGING IN LITIGATION, PART TWO: *HERZIG V. ARKANSAS FOUNDATION FOR MEDICAL CARE, INC.*

A. Background of the Case

Herzig v. Arkansas Foundation for Medical Care, Inc. was a case involving age discrimination of two previous employees of Arkansas Foundation for Medical Care, Inc. (AMFC), a nonprofit that provides "medical necessity review services" regarding Medicaid through a contract with the State of Arkansas.[50] Plaintiff Brian Herzig was a Software Applications Developer and Director of Information Technology at AMFC.[51] Plaintiff Neal Martin worked as the Manager of Programming and Assistance Director of Information Technology at AMFC, and Martin reported to Herzig.[52] The employees were responsible for creating a software for AFMC that complied with HIPAA.[53] However, it came to light that their software had vulnerabilities and failed to ensure HIPAA compliance.[54] The employees were fired,[55] and later sued for age discrimination.[56]

"[T]he parties conferred pursuant to Federal Rule of Civil Procedure 26(f)" regarding the suit.[57] At this time, the plaintiffs agreed that AMFC could request data from their phones and agreed that they had "taken reasonable measures to preserve potentially discoverable data from alteration or destruction."[58] In response to AMFC's requests for production of "communications with current or former AMFC employees," the plaintiffs had only produced screenshots of some of their text messages—though these communications ended August 20, 2018.[59] By August 2018, both employees had downloaded an ephemeral messaging app, Signal, to their

---

[49] Philip J. Favro & Keith A. Call, *Focus on Ethics & Civility: A New Frontier in EDiscovery Ethics: Self-Destructing Messaging Applications*, 31 UTAH BAR J. 40, 40 (Mar./Apr. 2018).

[50] Herzig v. Arkansas Found. for Med. Care, Inc., No. 2:18-CV-02101, 2019 WL 2870106, at *2 (W.D. Ark. July 3, 2019).

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.* at *3.

[55] *Id.* at *4.

[56] Herzig, 2019 WL 2870106, at *4.

[57] *Id.*

[58] *Id.*

[59] *Id.*

phones.[60] Both employees turned on the message deletion option on the app and used it to communicate discreetly.[61] The plaintiffs did not furnish these messages in discovery, and AMFC only became aware that the plaintiffs were using Signal to communicate when Herzig mentioned their use of Signal in his deposition near the end of discovery.[62]

B. Regarding Spoliation of Evidence through Ephemeral Messaging

Unlike in *Waymo*, the court granted a spoliation motion in part in this case in response to a "motion to dismiss or order an adverse inference and bath faith spoliation of evidence."[63] The court considered the following facts in its ruling: (1) the plaintiffs were originally reluctant to comply with orders to turn over their text messages; (2) the plaintiffs only turned over their text messages in response to a motion to compel; (3) the plaintiffs then switched to an app capable of destroying communications and turned on the deletion setting, thus "intentionally act[ing] to withhold and destroy discoverable evidence"; (4) the plaintiff's "familiarity with information technology"; (5) the plaintiff's "initial misleading response" that Martin did not have any responsive communications; and (6) the plaintiff's "knowledge that they must retain and produce discoverable evidence."[64] This information cumulatively persuaded the court that the plaintiff's use of ephemeral messaging—"decision to withhold and destroy communications"—was "intentional and done in bad faith."[65] As a result, the court held that Herzig and Martin had intentionally spoliated evidence in bad faith through the use of an ephemeral messaging app, and the request for sanctions was only denied because it was moot due to the granted motion for summary judgment.[66]

While courts will no doubt continue to wrestle with the thorny issue of spoliation sanctions arising out of the use of ephemeral messaging apps, the landscape is already shifting when it comes to the Department of Justice ("DoJ") investigations. Take the Foreign Corrupt Practices Act ("FCPA"), for example. Initially, FCPA was "enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business."[67] Since its adoption, the FCPA has grown to match

---

60 *Id.*

61 *Id.*

62 Herzig, 2019 WL 2870106, at *4.

63 *Id.*

64 *Id.* at *4–*5.

65 *Id.* at *5.

66 *Id.* at *7.

67 *Foreign Corrupt Practices Act*, DEPT. JUSTICE, https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.

the fast-paced evolution of technological advancements that could facilitate the activity it was enacted to protect.

In the age of high-tech corporate wrongdoing, what happens when in-house corporate employees begin utilizing ephemeral messaging with malicious intent? What happens when those "here today, gone today" conversations take place on company-provided cellular devices? Addressing this issue, the DoJ has carved out a niche allowing companies to self-disclose such activity in order to mitigate potential criminal investigations.[68]

The FCPA now allows for companies to receive leniency reductions from the United States Sentencing Guidelines (USSG) as far as only having to pay 25% of the lowest fine accorded by the USSG—absent egregious or recurring criminal activity—so long as remedial measures are "timely and appropriate."[69] The DoJ goes on to give examples of what, exactly, is "timely and appropriate" measures. Specifically, as it pertains to ephemeral messaging, the company must have "implement[ed] appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention polices or legal obligations."[70]

This particularly affects companies that provide their employees with cell phone devices to conduct business and poses quite a compliance department challenge to meet the aforementioned FCPA leniency guidelines.

Common sense dictates that perhaps the best policy a company can adopt is simply to not allow the download of these types of applications to an employee's business phone. Of course, due to the technological savvy of the new generation of workforce, that is much easier said than done. Also, there has yet to be a public declination issued under the new FCPA policy that has cited a company's prohibition on ephemeral messaging software as a basis for conferring full credit for remediation.[71]

Questions remain. How can companies wrestle with some of the most popular ephemeral messaging apps—and their appeal—and avoid civil and DoJ pitfalls waiting in the wings? For

---

[68] Sec. 9-47.120 - FCPA Corporate Enforcement Policy Manual.

[69] *Id.* at 1 (Credit for Voluntary Self-Disclosure, Full Cooperation, and Timely and Appropriate Remediation in FCPA Matters).

[70] *Id.* at 3. c. (Timely and Appropriate Remediation in FCPA Matters).

[71] *DOJ Revises Policy on Instant Messaging App in Foreign Corrupt Practices Act Enforcement*, BLOOMBERG L., *in* ROSMAN ET AL., RETAINING EPHEMERAL MESSAGES TO PREPARE FOR DOJ SCRUTINY (2019).

companies to be effective, they must admittedly provide their employees with the best feasible technology, and many times this requires the issuance of a company cell phone.

Enter, compliance departments. The FCPA provides a bulleted outline of measures that compliance departments can take to help keep themselves out of hot water. Among other items, the DoJ will look to the company's culture of compliance, resources dedicated, authority and independence of compliance departments to audit employees, and compensation of compliance personnel when making a determination of remediation.[72] These, among other measures, will play a role in prosecutorial discretion if and when the DoJ suspects criminal activity is afoot and begins investigating.

In the age of the COVID-19 pandemic, with a sizeable portion of the Fortune 500 companies working from home, these issues draw even more attention. Recently, the CEO of Twitter announced that his entire work force was welcome to work from home in perpetuity.[73] In this unprecedented age where technology is so heavily relied upon to maintain productivity, regulation and compliance reviews will continue to be imperative. Messages may disappear, but liability always remains.

---

[72] FCPA Corporate Enforcement Policy Manual, *supra* note 68, at c (Timely and Appropriate Remediation in FCPA Matters).

[73] Dylan Byers, *Twitter employees can work from home forever, CEO says*, NBC News (May 12, 2020), https://www.nbcnews.com/tech/tech-news/twitter-employees-can-work-home-forever-ceo-says-n1205346.

About the Authors

John Browning is an attorney in Dallas who litigates a wide variety of civil litigation in state and federal courts throughout Texas, including commercial disputes, personal injury and wrongful death defense, employment matters, health care, and intellectual property litigation. He is the author of the books The Lawyer's Guide to Social Networking, Understanding Social Media's Impact on the Law, (West 2010); the Social Media and Litigation Practice Guide (West 2014); Legal Ethics and Social Media: A Practitioner's Handbook (ABA Press 2017); and Cases & Materials on Social Media and the Law (forthcoming). Mr. Browning is also a contributing author to seven other books, the author of nearly 35 published law review articles; and the award-winning writer of numerous articles for regional and national legal publications. His work has been cited in nearly 350 law review articles, practice guides in 11 states, and by courts in Texas, California, Maryland, Tennessee, New York, Florida, Illinois, and Puerto Rico. He has been quoted as a leading authority on social media and the law by such publications as The New York Times, The Wall Street Journal, USA Today, Law 360, Time Magazine, The National Law Journal, the ABA Journal, WIRED Magazine and Inside Counsel Magazine, and he is a recurring legal commentator for the NBC, CBS, and FOX news stations in Dallas. He is an adjunct professor at SMU Dedman School of Law and he serves as the Chair of the Computer & Technology Section of the State Bar.

W. Grant DuBois is an attorney at Suzanne Calvert & Associates, Employees of the State Farm Mutual Automobile Insurance Company, and former Assistant District Attorney for the State of Texas. His practice is dedicated to analyzing complex issues for his clients while maintaining his "always ready for trial" approach to litigation. DuBois is dual-licensed in Texas and Arkansas, and enjoys spending time with his young family and analyzing issues evolving from technology and litigation. Any opinions expressed in this article are his alone, and do not necessarily reflect the views of State Farm or any of its officers, employees, agents, subsidiaries, or affiliates.

Katherine Frisbee is a Dean's Scholar and third-year law student at SMU Dedman School of Law. She is a 2018 honors graduate of Emory University.

Everything You Always Wanted to Know About the CIPP/US Exam (But Were Afraid to Ask)

By Kristen Knauf

With dozens of headlines each week discussing the sharing of health data to help control the spread of COVID-19, examining the unintended uses of personal data collected by the latest technological gadgets, or just announcing yet another data breach at a Fortune 500 company, perhaps you have started to develop an interest in data privacy.

The International Association of Privacy Professionals ("IAPP") is a non-profit organization that helps support and improve the global community of privacy law professionals. As part of their mission, IAPP offers certification programs designed to demonstrate comprehensive knowledge of privacy laws and regulations and how to apply them to industry frameworks. One of these certifications is the Certified Information Privacy Professional (CIPP), which tests understanding of broad global concepts of privacy, jurisdictional laws, regulations and enforcement models, and legal requirements for handling and transferring data. There are four CIPP concentrations, each one focused on a specific region: Asia, Canada, Europe, and the United States (US).

I am proud to share that I recently passed the CIPP/US exam. For an exam so heavily focused on information sharing, however, I found there to be a surprising lack of information about the test experience itself and how one should best prepare. If your budding interest in data privacy has you considering an IAPP certification, here is my advice for anyone who may be considering taking the CIPP/US exam:

1. Read the Materials.

IAPP provides two free documents that tell exam takers what to study. The first is a "Body of Knowledge" that outlines the five sections of the exam and lists all of the topics that could be covered under each section. But not all topics or sections are tested the same. This leads to the second document, the Exam Blueprint which states how many questions may appear under each section. Given how quickly the relevant data privacy laws are changing, make sure that you have the most updated version of the Body of Knowledge and Exam Blueprints.

My preparation consisted of reading two textbooks and completing a series of practice exam questions. The first book was the official IAPP CIPP/US textbook. The second was an unofficial study guide that I purchased from Amazon. I read the official textbook in its entirety once while highlighting the crucial points. I then went back and re-read the chapters covering

medical data, financial data, and workplace privacy. While I skimmed the content in the study guide, the study guide's real value was in its dozens of practice questions that were incredibly helpful in confirming my understanding of the broader concepts and remembering details of the particular state and industry-specific regulations. IAPP sells sample questions, although sometimes IAPP will offer sample questions (and other resources) for free if you are on their email list.

2. Pay Attention to Details.

Unlike other countries that are governed by one omnibus data protection regulation (i.e. GDPR), the United States has a patchwork of federal and state laws that cover data privacy. When concentrating on the federal and industry-specific U.S. laws, I found it helpful to focus on the following details:

- Scope – Who and what type of information is covered? And why?
- Enforcement – Who enforces the law? Are violations criminal or civil? Is there a private right of action for individuals?
- Penalties – What happens when there is noncompliance?
- Preemption – Does federal law preempt state law?

It is also helpful to study what may seem like arbitrary facts about these laws. Questions like "CALEA is also known as _____" are silly, but fair game (the answer is the Digital Telephony Act).

Regardless of which state(s) you practice in, do not gloss over the details of state-specific privacy laws. Questions on the California Consumer Privacy Act are expected, but the test also covers the little nuances of most of the major state breach notification laws (specifically, California, Texas, Illinois, Tennessee, New Mexico, Delaware, Massachusetts, and Maryland, as each of these states has their own interesting privacy flair in their breach laws).

3. Take Your Time.

By "take your time" I mean both in preparing for the exam and on the exam itself. IAPP recommends that you "train and study for a minimum of 30 hours." My work and interest in this area already had me reading news articles, journal articles (including past issues of *Circuits*!), and blog posts that discussed data privacy laws. It goes without saying that the greater your interest in the subject matter, the easier it will be to retain the textbook material without rote memorization. Yet, it is impossible to obtain a solid understanding of the topics

by simply reading news articles and skimming the study guide, and I probably spent 30-40 hours spread out over a couple of months reading the textbooks and reviewing practice questions before taking the exam.

The exam itself was, in a word, odd. It consisted of 90 multiple-choice questions, 75 of which were scored, and 15 of which were non-scored "experimental" questions. The questions alternated between being so easy that they felt like a joke to maddeningly tricky "EXCEPT" questions that included double negatives and required two or three readings. Put another way, the CIPP was similar to the MPRE: the material was not difficult per se, but the question style can trip you up if you are careless. The good news is that with 150 minutes to take the exam, you have a little more than a minute and a half per question. Go slow and read the questions carefully. Like many standardized tests, there is no penalty for incorrect answers, so be sure to answer every question on the exam.

The CIPP/US exam is nowhere near as difficult as the bar exam. The exam's structure and novelty, however, may make it seem more daunting. My best advice is to put in the time to read the official textbook, complete any practice questions that you can find, and take your time reading and working through the questions on the exam itself. Because the exam is computer-based, your results are provided visually on the computer screen immediately after completion. Once you pass the CIPP/US, you can get back to worrying about other privacy-related issues, such as how much your Amazon Echo has really been listening to your conversations. Good luck!

About the Author

Kristen Knauf is a Senior Attorney at the American Heart Association. She is a council member of the Computer and Technology Section of the State Bar of Texas (2017-20). She received her JD from Marquette University and holds bachelors degrees in Spanish and Political Science from the University of Wisconsin.

The COVID-19 Crisis and the Move Toward Online Notarization

By Kirsten Kumar

Given the effect that COVID-19 has had in bringing many legal processes and business transactions to a temporary halt, we all have sought ways to adapt some of life's rhythms and procedures to the virtual world, from virtual work happy hours to the Texas Supreme Court's hearing of oral arguments via Zoom.[1]

This has been no less true for individuals who are in the midst of processes requiring notarized documents, especially as people are scrambling to ensure their estate plans are properly in place. As courts, law firms, and businesses adapt to working remotely, there has been a significant uptick in interest in using online notarization across the U.S.

Common Forms of Online Notarization

Perhaps most common of the forms of online notarization is Remote Online Notarization, or "RON": the online equivalent of a traditional paper-based and in-person notarization.[2] RON differs from electronic notarization, or eNotarization, which maintains an in-person requirement but includes electronic signatures on documents in an electronic form.[3] In contrast, every part of the notarization process in RON is done using two-way audio-video technology. A physical stamp is replaced with an electronic notary seal and the notary public's signature is replicated by a digital certificate.

Also uniquely different from RON is RIN, or Remote Ink-Signed Notarization. While RON uses a dedicated software that integrates video-conference ability with methods for identify verification and electronic signature of electronic documents in real-time, RIN is typically conducted by video-conference platforms such as Zoom, WebEx, or Microsoft Teams and consists of paper documents signed in ink and faxed or electronically transmitted between the

---

1 Chuck Lindell, *In a first, Texas Supreme Court goes live on YouTube*, STATESMAN (Apr. 8, 2020), https://www.statesman.com/news/20200408/in-first-texas-supreme-court-goes-live-on-youtube.

2 *What is remote online notarization?*, NATIONAL NOTARY ASSOCIATION, https://www.nationalnotary.org/knowledge-center/remote-online-notary/how-to-become-a-remote-online-notary.

3 Michael Lewis, *Remote Notarization: What You Need to Know*, NATIONAL NOTARY ASSOCIATION (updated May 21, 2020), https://www.nationalnotary.org/notary-bulletin/blog/2018/06/remote-notarization-what-you-need-to-know.

signer and Notary.[4] While RIN is a significant step in expediting notarization in a time of crisis, there are further implications to be considered by both the Notary and signer, including the security of the video-conference platform, a secure backup of the notarization, and the potential misconception that can arise from a signer looking through pages of a paper document outside the physical presence of the Notary.[5]

However, those seeking to use RON or RIN should be aware: permissible practices in remote notarization varies among states. Some states only allow RIN, while others permit RON using only specified software, and still others prohibit online notarization in its entirety. Individuals considering using RON should look into the applicable laws of their jurisdictions to ensure compliance, especially given recent rapid developments in state statutes on online notarization.

States with Permanent Online Notarization Laws

Online notarization methods have seen increased interest as tools to be used during the limitations in place due to COVID-19, but some states have allowed the use of such methods far before this pandemic. Twenty-four states currently have statutes in place authorizing online notarization, including Texas.[6] Additionally, Arizona, Iowa, and Nebraska have each enacted legislation to allow online notarization, effective July 1, 2020. Maryland and Washington have similar legislation in place, effective October 1, 2020; and Alaska's statute allowing RON will be effective January 1, 2021.[7]

States Taking Emergency Action for Online Notarization in Light of COVID-19

Although only about half the states in the U.S. have permanent online notarization statutes in place or set to go into effect in the future, some form of online notarization is currently permissible in a majority of states. Many states (and the District of Columbia) have enacted emergency authorization for online notarization given the social distancing standards in place.

Some states, like Florida and Texas, issued emergency measures in addition to the permanent online notarization laws already in place. For example, Florida's emergency measures

---

4 Bill Anderson, *10 Standards Of Practice For Remote Ink-Signed Notarizations* (updated Apr. 20, 2020), https://www.nationalnotary.org/notary-bulletin/blog/2020/04/10-standards-video-conference-notarizations.

5 *Id.*

6 Michael Lewis, *Remote Notarization: What You Need to Know*, NATIONAL NOTARY ASSOCIATION (updated May 21, 2020), https://www.nationalnotary.org/notary-bulletin/blog/2018/06/remote-notarization-what-you-need-to-know.

7 *Id.*

authorized any Notary public to administer oaths for court proceedings remotely, regardless of whether they had completed the required online notarization training.[8] Other states, such as Alabama, Massachusetts, and New York, issued orders allowing temporary RON or RIN, New York being the first state to issue an executive order allowing RIN.

Online Notarization in Texas

Texas was the third state to adopt a statute allowing online notarization by passing Texas Government Code Section 406.101 *et seq*, effective as of July 1, 2018.[9] When commissioned, an online Notary is authorized to sign as online notarizations any instruments related to the acknowledgment or proof of written instruments, the protestation of certain instruments, the administration of oaths, the taking of depositions, and the certification of copies of documents not recordable in public records.[10] Further, an online Notary can perform an online notarization even if the principal is not physically located in Texas at the time of the notarization.[11] The online Notary, however, must physically be in the state.[12]

In many respects, the online notarization procedure does not differ drastically from the traditional procedure. Texas allows for remote verification of an individual's identity through the online Notary's personal knowledge of the individual, credential analysis, identity proofing, or by the individual's remote showing of a signed government-issued photo I.D.[13] Additionally, the Notary is required to maintain an electronic record for every online notarization for at least five years under the Statute.[14]

On April 8, 2020, Texas Governor Greg Abbott temporarily suspended certain statutes to allow for appearance before a notary public via video-conference link to execute certain estate planning documents, including a self-proved will, a durable power of attorney, a medical power of attorney, a directive to physician, and an oath of an executor, administrator, or guardian. This suspension will remain in place until the Office of the Governor terminates it or

---

8 *States Take Emergency Action On Remote Notarization And Signers' ID*, NATIONAL NOTARY ASSOCIATION (Mar. 25, 2020), https://www.nationalnotary.org/notary-bulletin/blog/2020/03/states-emergency-action-remote-notarization.

9 David Fowler Johnson, *Notary Services In A World of Social Distancing: Online Notarization*, THE NAT'L L.R. (Apr. 7, 2020), https://www.natlawreview.com/article/notary-services-world-social-distancing-online-notarization.

10 4 TEX. GOV'T. CODE § 406.107 (2018).

11 *Id.* § 406.110(a).

12 1 TEX. ADMIN. CODE § 87.41(c) (2018).

13 4 TEX. GOV'T. CODE § 406.110(b)(2) (2018).

14 *Id.* § 406.108(c).

the March 13, 2020 state of disaster declaration is lifted or expired.[15] Under this Executive Order, any Texas Notary, whether a registered Online Notary or not, can perform a notarial act under the terms of the Order, as opposed to under the terms of the Government Code.[16]

On April 27, 2020, the Governor further temporarily suspended Section 121.006(c)(1) of the Texas Civil Practice & Remedies Code to allow certain real estate instruments to be acknowledged via video-audio technology. While this was originally set to terminate on the earlier of May 30, 2020 or the lifting of the declaration of state of disaster, it was recently extended until the earlier of the lifting of such declaration or June 30, 2020.[17]

Measures Taken by Congress to Permit Online Notarization Across States

Notably, individual state measures authorizing online notarization may not be necessary for much longer. On March 18, 2020, Senate Bill 3533, the Securing and Enabling Commerce Using Remote and Electronic Notarization Act of 2020, was introduced. This bill would authorize remote online notarizations across the U.S. and put in place standards for remote and online notarization that take place as part of or affect interstate commerce.[18] The substantially similar counterpart to Senate Bill 3533, H.R. 6364, was introduced in the House on March 23, 2020.[19]

While this bill has not yet become law, it would allow for online notarization to be conducted across the U.S. and would potentially have a significant impact on the frequency of traditional in-person notarizations. Given the increasing familiarity with video-conference many U.S. residents have experienced these last few months given the effects of COVID-19, online notarization may actually feel more comfortable to many users than ever before.

---

[15] Texas Secretary of State, Notice of Suspension of Statutes, *available at:* https://www.sos.state.tx.us/statdoc/notary-public.shtml (last visited May 30, 2020).

[16] TX Governor Executive Order, NATIONAL ROTARY ASSOCIATION, *available at:* https://www.nationalnotary.org/knowledge-center/news/law-updates/tx-governor-executive-order-2020.

[17] Office of the Attorney General, Notice of Extended Suspension of Statute, *available at:* https://www.sos.state.tx.us/statdoc/extended-suspension-of-statute.shtml (last visited May 30, 2020).

[18] S. 3533, 116th Cong. (2020).

[19] H.R. 6364, 116th Cong. (2020).

About the Author

Kirsten Kumar is starting her third and final year at the University of Texas School of Law and is currently interning for an international criminal tribunal at The Hague during the summer. Prior to starting law school, she was part of the technology community of Austin and worked in marketing for a local startup that was featured on ABC's Shark Tank. There, she created public-facing messaging, managed content marketing and assisted in producing content for the startup's pitch in SXSW's 2016 Accelerator Pitch Event, which it won.

Kirsten has a background in multimedia journalism, including digital photography, videography, and graphic design and has been published in various media, including lifestyle magazines and KUT Austin radio, an NPR affiliate. In addition to tech and IP, Kirsten has experience in immigration law and an interest in international humanitarian and human rights law, which she hopes to pursue upon completing her law degree.

A Gentle Introduction to AI: With a Useful Example

By Ronald L. Chichester[1]

> It is very nearly a principle of nature that where law seeks to keep pace with technology, technology wins. It is like a race between an ox cart and a supersonic jet.
>
> — Theodore Roszak[2]

Lawyers are often tortured with bad software. Sadly, most software companies think lawyers are rich and ripe targets for shoddy applications. Fortunately, there are ways (now) that lawyers can start to take command of the technologies that they use to generate work product. Done correctly, the employment of technology, and in particular artificial intelligence ("AI"), can be a significant help to attorneys and judges alike.[3] "Correctly" means taking small steps. As the old adage goes, you have to walk before you run. This short article will introduce a simple AI process that can shave seconds to minutes off the time needed to identifying legal areas in documents. Don't scoff at saving a few seconds. They add up. Remember, once the small steps are mastered, you'll find ways to pick up speed. Moreover, the technology described herein can be incorporated into other software applications in order to enhance them. It is the incorporation of AI into existing tools that makes AI particularly powerful for lawyers.

The technology for this article will be about *text summarization*.[4] For this article, text summarization is defined as producing a shorter set of text that represents the most important elements of a larger set of text. The idea is that the AI summarizes a legal document, and gives a short subset of the text that enables the attorney to quickly determine if more attention to the original document is warranted.

---

[1] Ron is a solo practitioner in Frisco, Texas (with a country office in Nacodoches County). He would like to thank Mr. Joseph Jacobson of Dallas for some very helpful comments about this article.

[2] THEODORE ROSZAK, THE CULT OF INFORMATION: THE FOLKLORE OF COMPUTERS AND THE TRUE ART OF THINKING (1988). While the context for that observation was surveillance, that observation has much broader applicability.

[3] For a (short) list of example AI-based legal applications, *see*, Daniel Faggella, *AI in Law and Legal Practice – A Comprehensive View of 35 Current Applications*, EMERJ (Mar. 14, 2020), https://emerj.com/ai-sector-overviews/ai-in-law-legal-practice-current-applications/.

[4] For an introduction into the technology of text summarization, see Jason Brownlee, *A Gentle Introduction to Text Summarization*, MACHINE LEARNING MASTERY (last updated Aug. 7, 2019), https://machinelearningmastery.com/gentle-introduction-text-summarization/.

Text summarization comes in two varieties: textual and visual. Both include words, obviously, but what is presented, and how those words are presented, differs significantly. The visual representation is referred to as a "wordcloud" or, in data science parlance, "bag of words." The textual representation is often referred to as "text summarization."

We start with an example document, which in this case is a master services agreement.[5] It is five pages long, and is replete with legalese. Perfect for this demonstration.

There are several online tools to generate wordclouds; many of which are free to use. One example is Wordclouds.com.[6] Simply input the text of the document, and it will generate a wordcloud as shown in Illustration 1.

Illustration 1: Wordcloud of the Master Services Agreement

As you can see from the illustration, the key words are larger than the remaining text because those words form a larger percentage of the corpus of the document. If you want to discern quickly the *type* of legal document, then wordclouds can be just the thing because "company," "services," "agreement," "sow," and "deliverable" are all prominent and indicative of a master services agreement. Wordclouds may also be employed to identify the legal areas in a court opinion to speed up research tasks. Some attorneys even use wordclouds in conjunction with document discovery.

---

[5] This document was taken from a website that provides basic templates for contracts. In this case, we're using a Master Services Agreement, which is available at: https://www.docracy.com/0gjm5qhy1nv/master-services-agreement.

[6] Wordclouds, https://www.wordclouds.com/.

For standard (textual) text summarization, there is another set of online tools. It should be noted that text summarization is a difficult task—one that has taxed the limits of data scientists. Over the years, different types of artificial intelligence have been employed, with varying levels of success. The first attempts were comical. Lately, however, the summarizations have proven themselves to be useful tools. One such (free) online tool is the "Online Text Summary Generator"[7] which is free to use. The easiest way to use that tool is to load the document into a word processor, then copy the whole document and paste it into the appropriate box on the website. You can select how many paragraphs the document should be condensed to (the default is five). For this article, the five-page master services agreement was condensed down to five paragraphs, namely:

> "Company shall provide services for purposes of to the Client as described on one or more Statements of Work signed by Company and Client that reference this Agreement. Company shall perform Services in a prompt manner and have the final or service ready for Client no later than the due date specified in the applicable SOW.
>
> If additional SOW are executed, then Client shall pay Company for all services performed prior to the additional SOW before Company begins work on the new SOW. Termination. Company shall have the right to modify, reject, or terminate any SOW and any related work in process with five days written notice to Client. In the event Company terminates the SOW prior to completion of Services, the Client shall pay Company the fees due under the SOW with respect to Services completed as of the date of termination.
>
> Upon settlement of funds due to Company, all Client provided materials will be returned to Client and all Client use rights in the work in process as described in Section 9 will be transferred to Client.
>
> In exchange for Companys Services under this Agreement, the Client shall pay Company the contract price and deposit set forth above. Company will submit a final invoice to Client for all services rendered by the Services Completion Date and Client shall promptly pay. Client is restricted from using any form of the Deliverable until final payment is received."

[7] Automatic Text Summarizer, https://autosummarizer.com/index.php.

While it wouldn't get an "A" from your grammar teacher, the summarization does convey enough information—even in the first paragraph—to correctly identify the document as a services agreement. You might ask: "Can you make a wordcloud out of the text summarization?" Of course, and such a wordcloud would look something like:

Illustration 2: Wordcloud of the Text Summarization

Again, useful, and perhaps easier to discern than the first wordcloud. That's an illustration of "piping" two tools together to make a better result. Since these tools are based on open source technologies,[8] they are ripe for integration into existing software applications. For example, this form of AI could be integrated into a file manager, so that when you click on a document, it shows both the wordcloud and the text summarization, as demonstrated in Illustration 3.

[8] You can read about open source software at *What is open source?*, https://opensource.com/resources/what-open-source.

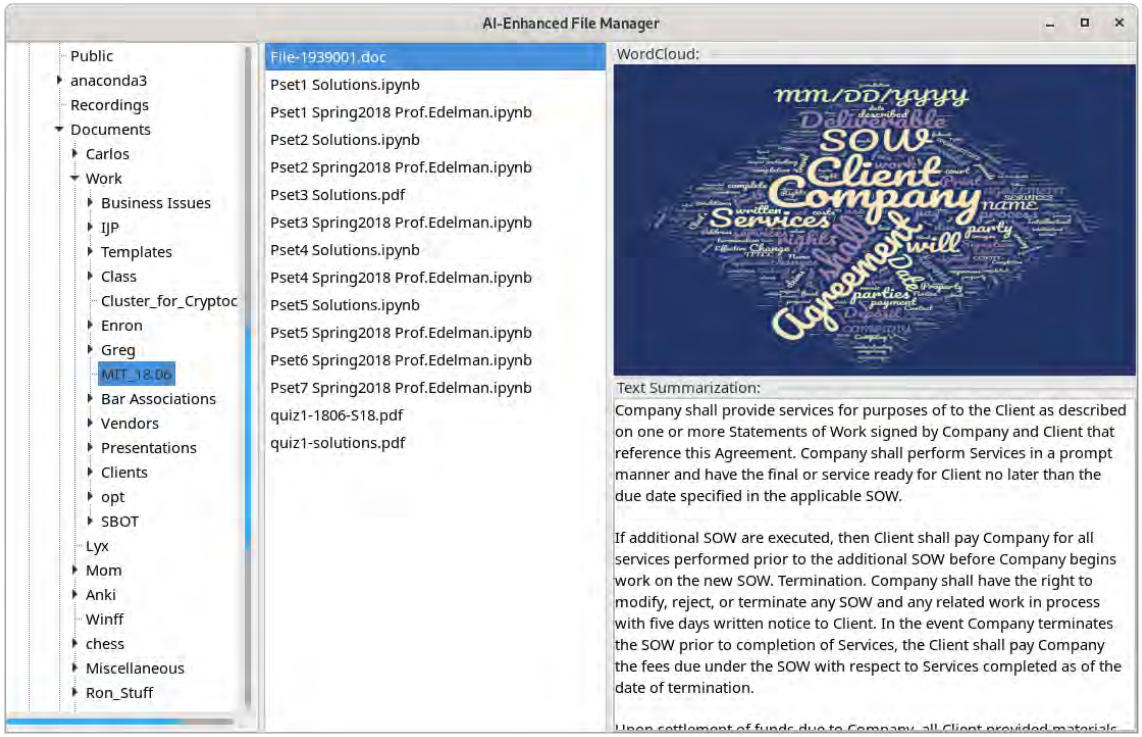


Illustration 3: File Explorer with AI Integration

Given the advances in AI, it is unsurprising that some AI has been created for specific types of legal documents. An example (that is available under an open source license) is called LexNLP, and is part of the ContraxSuite application.[9] LexNLP is an "extraction tool for real, unstructured legal text," particularly contracts.[10] LexNLP utilizes a branch of technology called "natural language processing" that automates the parsing and categorization of words in legal documents like contracts and court opinions. It employs pre-trained models to recognize pages and sections within documents, as well as dates and duration, court citations, regulations, monetary amounts (*e.g.*, for royalties), conditions (*e.g.*, "less than" or "later than") and more. Could you use something like LexNLP to parse millions of words in thousands of documents? The answer is, "Yes." Some software companies do this as a service (with a fee). However, attorneys have started using open source software to do the same thing for free, which gives those attorneys a price advantage over their brethren.

As for the "state of the art" in text summarization, OpenAI[11] just released a beta version of its API product.[12] According to the website, the API can apply "to any language task — semantic

---

9 ContraxSuite, https://contraxsuite.com/.

10 LexNLP, https://contraxsuite.com/lexnlp/.

11 OpenAI, https://openai.com.

12 OpenAI technology, just an HTTPS call away, https://beta.openai.com/.

search, summarization, sentiment analysis, content generation, translation, and more — with only a few examples or by specifying your task in English."[13] More importantly, the "API allows searching over documents based on the natural-language meaning of queries rather than keyword matching."[14] One tech observer stated:

> "Over the past few months, OpenAI has vacuumed an incredible amount of data into its artificial intelligence language systems. It sucked up Wikipedia, a huge swath of the rest of the internet and tons of books. This mass of text -- trillions of words -- was then analyzed and manipulated by a supercomputer to create what the research group bills as a major AI breakthrough and the heart of its first commercial product. . . ."[15]

In summary, there are some remarkable technologies that are available right now to help automate some of the more tedious chores for attorneys and their staff. However, the attorney must make some accommodation with the *presentation* of the information that AI provides if the attorney is to make proper use of that information. Humans, however, excel at adaptation. The AI illustrated here won't take your job, but it can make your job easier and leave you more time to do what humans do best.

About the Author

Ronald Chichester is a solo attorney in the Dallas area who specializes in computer-related legal areas, including artificial intelligence, blockchains, smart contracts, distributed autonomous organizations, data privacy & regulation, as well as all aspects of intellectual property. Ron is the Chair of the Blockchain and Virtual Currencies Committed of the Business Law Section of the Texas Bar, and is a past chair of both the Business Law Section and the Computer & Technology Section.

---

[13] *Id.*

[14] *Id.*

[15] Msmash, *Trillions of Words Analyzed, OpenAI Sets Loose AI Language Colossus,* SLASHDOT (June 11, 2020), https://slashdot.org/story/20/06/11/1813258/trillions-of-words-analyzed-openai-sets-loose-ai-language-colossus.

A little-known aspect of the French Data Protection Act

By Pierre Grosdidier

Long before the Internet and GDPR, when disco ruled the airwaves, French legislators recognized that information technology threatened privacy and enacted a law commonly called the *Loi informatique et libertés*, which the French now call their Data Protection Act.[1] This pioneering law was one of first in Europe and has undergone substantial revisions since its first enactment.[2] The current version is quite long (128 articles) and incorporates the European Union's GDPR. This article discusses only an aspect of this law that is relatively little-known within U.S. legal circles, namely the limits that exist on the collection of personal data.

The law's Article 1 sets the tone and places computing in relation to human rights. Article 1 states, in part:[3]

> Computing must be at the service of every citizen. Its development must take place within the framework of international cooperation. It must not infringe on human identity, human rights, privacy, individual or public freedoms.[4]

Article 2 broadly defines "personal data files," meaning files that contain personal data.

> A personal data file is any structured set of personal data accessible according to determined criteria, whether this set is centralized, decentralized or distributed functionally or geographically.

---

[1] Law No. 78-17 of Jan. 6, 1978, relative à l'informatique, aux fichiers et aux libertés, Journal Officiel de la République Française [J.O.] [Official Gazette of France], Jan. 7, 1978, p. 227. The name of the law translates literally as "Law relative to computing, files, and liberties." The web site of the Commission Nationale de l'Informatique et des Libertés, which enforces the law, uses the name French Data Protection Act, which accurately conveys the law's intent. The term "databases" would be more apt today than the word "files." Also, the French term "*informatique*" can be variously translated as "computing," "computer science," or "information technology."

[2] But not *the* first.

[3] The translations are mine with the help of Google Translate.

[4] This juxtaposition of computing and human rights might initially surprise a non-French. Anecdotal evidence suggests that it was inspired in part in response to the Vichy regime's despicable use of *fichiers* (files) to nefarious ends during the Occupation.

Article 4 specifies the conditions under which personal data can be collected. Personal data must be, in part:

1° Processed lawfully, fairly and, for processing under Title II, transparently to the concerned person;

2° Collected for specific, explicit and legitimate purposes, and not to be further processed in a manner incompatible with these purposes.

Other restrictions apply. The law limits collected data to what is required for their ends and only for as long as necessary to meet those ends. The data must be correct, kept up to date, and kept secured. The key point is that personal data must be collected *for a legitimate reason*, and only to the extent necessary to fulfill this legitimate reason. Likewise, Article 5 restricts the conditions under which personal data can be processed to those where there is either consent by the owners of the personal data or a legitimate reason. For example, a neighborhood butcher who keeps a list of customer names with their outstanding balances probably stays within the law because the list and its numbers are for a legitimate and specific reason, *i.e.*, debt collection. But, the butcher likely strays from the law if he transcribes this list to an Excel file and adds information and comments regarding the customers' ability to pay, like the model of the cars they drive, where they work, their external signs of luxury like designer watches or purses, etc.[5]

In July 2018, the *Commission Nationale de l'Informatique et des Libertés* ("CNIL") fined a public housing entity in the city of Rennes (Britany) 30,000 euros because it illicitly used its tenant records.[6] The entity used these records to distribute a politically-motivated letter that protested the French government's plan to reduce housing subsidies. In its decision, the CNIL reiterated that, under the French Data Protection Act, personal data must be collected for "specific, explicit and legitimate" purposes, and that the use of tenant personal data to distribute a political letter manifestly did not qualify as a legitimate use.

Per the law's Article 6, and subject to exceptions,

---

[5] This example is inspired from an actual case reported in the French press at least 20 years ago.

[6] Press release, OPH de Rennes : sanction pécuniaire pour une utilisation du fichier des locataires incompatible avec la finalité initiale, CNIL (Jul. 31, 2018), https://www.cnil.fr/fr/oph-de-rennes-sanction-pecuniaire-pour-une-utilisation-du-fichier-des-locataires-incompatible-avec.

> [i]t is prohibited to process personal data that reveal alleged racial or ethnic origin, political opinions, religious or philosophical beliefs or the trade union membership of a natural person or to process genetic data, biometric data for the purpose of uniquely identifying a natural person, data relating to health or data relating to the sexual life or sexual orientation of a natural person.

In September 2018, the CNIL assessed a 10,000 euro fine against an employer that had used employees' fingerprints to record and track their clocking times.[7] There were other issues with phone calls that were recorded without employees' knowledge and insufficiently robust passwords. Last year, the revelation that an entity acting for Monsanto had been tracking in a spreadsheet the opinions of a couple hundred public personalities (half of whom were journalists) regarding the herbicide glyphosate caused an uproar in France.[8] The revelation spurred an apology from Bayer, Monsanto's owner, formal judicial complaints by journalists, and calls for the CNIL to investigate.[9]

The CNIL-assessed administrative fines can bite.[10] Article 21 caps fines at 10 million euros or, for a company, 2% of world-wide revenue for the previous financial year (or twice these amounts under the GDPR's Article 83). In November 2019, a company that tele-marketed its home thermal insulation services was fined 500,000 euros for, *inter alia*, recording derogatory comments and comments regarding the health of solicited persons in their database, and for insufficiently informing these persons regarding the use of their personal data and their rights.[11]

Penal sanctions also apply, as specified in Articles 226-16 *et seq.* of the French Penal Code.

> The collection of data by a fraudulent, unfair or illicit means, or of carrying out processing of personal information concerning a natural person without the

---

7 Press release, Biométrie au travail illégale : sanction de 10.000 euros, CNIL (Sept. 20, 2018), https://www.cnil.fr/fr/biometrie-au-travail-illegale-sanction-de-10000-euros.

8 Gérard Haas & Axelle Poujol, Fichage en secret de personnalités : l'affaire Monsanto, HAAS Avocats, https://info.haas-avocats.com/droit-digital/fichage-en-secret-de-personnalites-laffaire-monsanto.

9 The CNIL did not return a request for comments.

10 *See generally*, Sanctions, CNIL, https://www.cnil.fr/fr/tag/Sanctions.

11 Press release, FUTURA INTERNATIONALE : sanction de 500 000 euros pour démarchage téléphonique illéga*l*, CNIL (Nov. 26, 2019), https://www.cnil.fr/fr/futura-internationale-sanction-de-500-000-euros-pour-demarchage-telephonique-illegal.

person's authorization, when this objection is based on legitimate reasons, is punishable by five years imprisonment and a fine of 300,000 euros.

Article 226-21 applies the same fines to the misuse of personal information. The take-away from this article is that it is essential to consult with an attorney knowledgeable in French privacy law before collecting and processing personal data in France.[12]

About the Author

Pierre Grosdidier is Senior Assistant City Attorney at the City of 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 Secretary for 2019-20. He was the Section's Webmaster and Circuits eJournal Co-Editor for 2018-19.

[12] The website La Quadrature du Net (available in French, English, and Spanish) is a good source of information regarding Internet and data privacy in Europe, and especially in France. The website's name is a pun on *la quadrature du cercle*, *i.e.*, the squaring of the circle.

USB Charging Perils: How Not to Get Juice Jacked

By Ronald Chichester

The "low battery" warning appears on your phone or tablet, right when you need to contact a client before a flight. The device needs a quick pick-me-up. No problem, the airport has a charging station with built-for-purpose USB charging ports. What could go wrong?

Plenty, say security experts. You cannot tell if the charging port will only charge your phone, or might instead try to connect to it to exchange data (malware in – client data out). Some innocent charging ports have data exchange functionality, and that's a danger to attorneys and clients alike. The problem is so prevalent that they have a name for it: *Juice Jacking*.

This phenomenon goes back to 2012, when a security researcher named Kyle Osborn posted a framework[1] on GitHub specifically for juice jacking.[2] That framework (and others like it) facilitate the development of software for juice jacking. Essentially, the unsuspecting victim simply plugs in their USB charging cable into what they think is a USB port. Unbeknownst to the victim, the charging port is actually a USB On-the-Go cable[3] that is connected to another device hosting the data-sucking malware.[4]

How do you prevent Juice Jacking? Although both iOS and Android have implemented security measures to mitigate the threat of juice jacking, there are some steps that attorneys can take to prevent juice jacking outright. The simplest solution is to use a "power-only" USB charging

---

1 Frameworks facilitate the development of software. Rather than writing common code from scratch to develop an application, developers will turn to pre-made frameworks to avoid "reinventing the wheel." *See, e.g.,* Wikipedia.org, Software framework, https://en.wikipedia.org/wiki/Software_framework.

2 *See* Github, https://github.com/kosborn/p2p-adb/. Note, Osborn did not invent juice jacking. The technique became known in the security community as early as 2011.

3 According to Wikipedia, "USB On-The-Go (USB OTG or just OTG) is a specification first used in late 2001 that allows USB devices, such as tablets or smartphones, to act as a host, allowing other USB devices, such as USB flash drives, digital cameras, mice or keyboards, to be attached to them. Use of USB OTG allows those devices to switch back and forth between the roles of host and device. A mobile phone may read from removable media as the host device, but present itself as a USB Mass Storage Device when connected to a host computer." Wikipedia.org, USB On-The-Go, https://en.wikipedia.org/wiki/USB_On-The-Go.

4 You can see an exposé created by NBCNews about Juice Jacking at: Joe Enoch et al, *Juice Jacking: Why you should avoid public phone charging stations*, NBC NEWS (Feb. 7, 2020), https://www.nbcnews.com/news/amp/ncna1132046. Juice Jacking was employed by criminals during episode 9, Season 1 of *CSI: Cyber* (April, 2015).

cable. You can get those at Amazon and other electronics stores.[5] Ironically, it is the USB cables that don't "guarantee data transfer" that are ideal for this situation because they *cannot* transfer data, and thus cannot subject your phone or tablet to juice jacking.

In addition to data-less cables, you can also purchase something called a USB condom (I'm not kidding).[6] Another alternative is to charge your phone with a power brick, and charge the power brick from the USB port (infected or not). Finally, you can always forgo the handy (potentially infected) USB port and use a plug with your own A/C power adapter. The latter option is likely your least-cost prohibitive alternative.

About the Author

Ronald Chichester is a solo attorney in the Dallas area who specializes in computer-related legal areas, including artificial intelligence, blockchains, smart contracts, distributed autonomous organizations, data privacy & regulation, as well as all aspects of intellectual property. Ron is the Chair of the Blockchain and Virtual Currencies Committed of the Business Law Section of the Texas Bar, and is a past chair of both the Business Law Section and the Computer & Technology Section.

---

[5] Search for "usb charging cable multiple adapters" and you'll find several examples. *See, e.g.,* Amazon.com, https://www.amazon.com/charging-Trendsetter-Multiple-Compatible-pack-Silver/dp/B0767CYH4W/ref=sr_1_1_sspa?crid=3M8SFKYYYCCQ2&keywords=usb+charging+cable+multiple+adapters&qid=1581526224&sprefix=multiple+adapter+charging+%2Caps%2C202&sr=8-1-spons&psc=1&spL.

[6] You can buy USB Condoms on Amazon and other retail electronic stores. *See, e.g.,* Amazon.com, https://www.amazon.com/USB-Defender-Transfers-Smartphone-Guaranteed/dp/B01MXRQ4TZ/ref=sr_1_2_sspa?keywords=usb+condom&qid=1581535180&sr=8-2-spons&psc=1&spLa=ZW5jcnlwdGVkUXVhbGlmaWVyPUFBWFFRNVpaU05QNlYmZW5jcnlwdGVkSWQ9QTAyNjUyMDdPU0s2NzQyNjNIMyZlbmNyeXB0ZW.

Automate My Practice

By Alex Shahrestrani

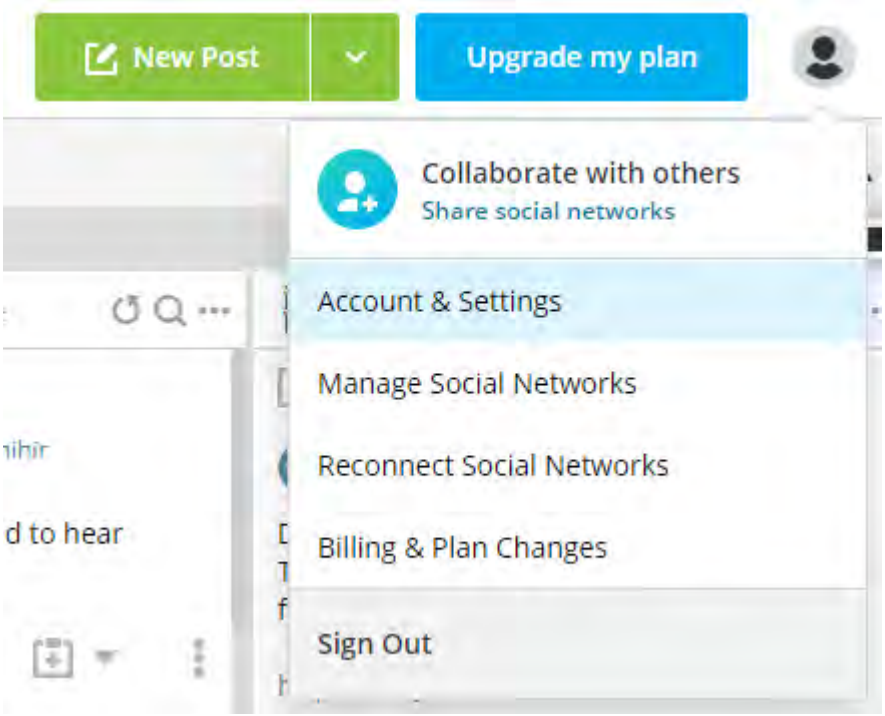
Hootsuite

This month, I'm going to show you how to automate social media posts using Hootsuite. Hootsuite is a tool which allows you to connect up to three social media accounts and schedule posts for up to a month out, all within the free version. If you're looking to increase your digital touch points with current and potential clients, or are looking for new ways to interact with your audience, Hootsuite is an easy way to start with great returns.

Initial Setup

To begin, you'll need to browse to hootsuite.com on your computer to make an account. Hootsuite lets you sign in using a social media account. I opted to sign in using Facebook because I wanted to connect my law firm's Facebook page to Hootsuite, and it saved me an extra step.

Once you've created your account, it's very simple to get started. Click on the avatar in the upper right corner of the screen to show the "Manage Social Networks" option and select it.



Next, you'll click on "+ Private Network" and add any additional networks you'd like to regularly post to. There are several options for integration, namely Facebook, Twitter, LinkedIn, Pinterest, Instagram, and YouTube. When you are connecting to a social network, you will need to authorize a personal account that manages your firm account. For example, I connected my personal LinkedIn account in order to get to my firm's LinkedIn account. Your setup may vary depending on a number of factors, but if you're a solo, it's most likely that connecting your personal account is the way to get to your firm account.

You can add up to three social media accounts under the free plan. If you ever need to change which accounts are publishing, you can go to the "Manage Social Networks" section and click on the gear next to the account you want to remove. It will pop up a menu which includes the option to "Remove from Hootsuite." You can then add a new account to your Hootsuite Dashboard.

Connect to Your Firm's RSS Feed

Once you have selected your preferred networks, you can get started with publishing content! If your firm's website has a blog that is at least semi-regularly published, then a good first step is to auto-publish your blog content whenever you create a new post.

Find Your RSS Feed

You'll need the link to your blog's RSS feed. If you have a blog section on your website, there's a good chance that you already have an RSS feed even if you don't know it. There are a few places to look for it: you can try "myfirmssite.com/feed", you can browse to your blog and look for the RSS symbol –  (that will be the link you need), or you can check your sitemap – probably "myfirmssite.com/sitemap.xml" – to see if the link is listed there. If that fails, I'd still wager that if you have a blog you have an RSS feed, and you can ask your webmaster or someone who is good with tech to help you find it.

Connect the RSS Feed to Hootsuite

Now that you have your RSS link ready to go, navigate to the menu on the sidebar and select the Publisher (). On the top bar menu of the Publisher page, select "Content." There will be a new menu on the left-hand side with a submenu called "Content Sources." Select "RSS Feeds" from the submenu, then click the plus sign to add a new feed.

Plug in your RSS Feed link and select which social media account you want it to connect to. There are some limitations on which accounts can connect here; there's no Twitter support for RSS feeds, and you have to connect the feed again for each social media network, but it's still a

worthwhile step. I leave the options at their default settings, but you can adjust those options if you are so inclined.

Scheduling Posts

Using the App

I prefer to schedule my posts directly from my phone or iPad, mostly because that's how I consume my content. However, there's an added bonus: you can "Auto Schedule" posts if you're using the app. Auto-scheduling is not available using the free version from the browser, but is included with the app for some reason.

It's as simple as sharing a post. When you come across an article you want to share, simply click on your device's share button and select the Hootsuite icon (). The first time you share, there will be an empty field, "Select a Social Network." When you click on that field, it will take you to a list of your connected social networks. If you think you will be regularly sharing to the same social networks whenever you post, then click on the pin button (📌) next to each of those networks. Doing so will add those networks for sharing the current content, and it will set the app up so those networks are selected by default for future posts.

After you've selected your social networks, you can edit your post to add your own comments or change the prefilled content in the provided box. The box will provide a character counter for each of your selected social networks so you know how close you are to the limit – a particularly useful feature for Twitter posts.

Once you're satisfied with your post, click the "Next" button: you might get a warning message, which you can generally ignore by clicking "Continue." You will be provided with three options, "Send Now," "Auto Schedule," and "Custom Schedule." The options are pretty self-explanatory: "Send Now" immediately shares the post, "Custom Schedule" allows you to pick a date and time for the post to go out, and "Auto Schedule" will set posts to go live at generally good posting times without overlapping your other scheduled posts. "Auto Schedule" will generally schedule no more than two posts per day, per social network, and will schedule on weekdays for roughly around 9am and 12pm.

"Auto Schedule" is most useful for creating a month of scheduled posts. You can set aside half an hour each month to go through content relevant to your audience and simply click your share button. I often intersperse old blog posts in the schedule to keep my content relevant to the audience. I use the "Share Now" option for content that isn't likely to be relevant later on,

and I use "Custom Schedule" for timed announcements or to target a specific event. An example of how I use "Custom Schedule" is to interact with SXSW. I help them with their Legal Education track, so I'll schedule posts that are thematically relevant to SXSW and my practice to generate buzz and benefit from the traffic that SXSW generates.

Using the Browser

Scheduling posts with the web browser is largely the same as using the app with a few differences.

The web browser won't automatically fill your preferred social networks into the field, though it's not difficult to select them yourself. It's just an extra step I prefer to avoid by using the app.

You will have to copy and paste the link that you'd like to share into the provided field, and the link won't auto-generate text for you like the app will.

You can select a date and time for the post, or you can share now; but the free version will not allow you to "Auto Schedule" from the browser.

Wrapping Up

There are other features that can be useful. There's a browser extension that you may want to try, but the above discussion should be enough to get you started with Hootsuite.

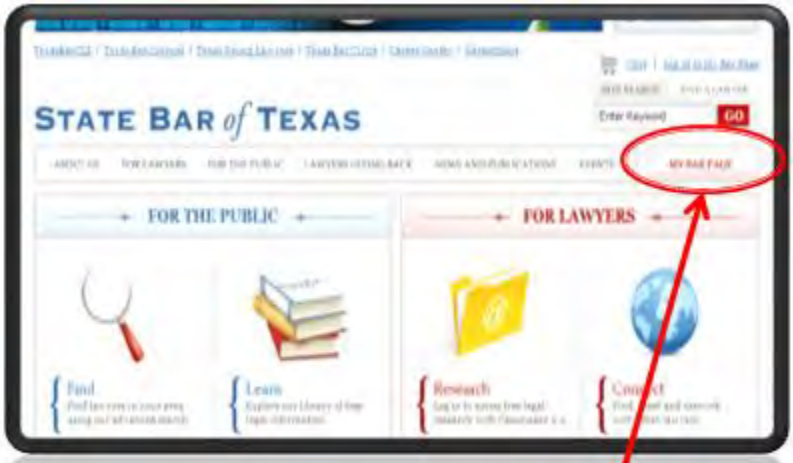
If you're looking for help with your setup, you can feel free to reach out to me at alex@shahrestanilaw.com, or find me on your favorite social network!

About the Author

Alex Shahrestani is a startup-tech nerd trapped in an attorney's body. He serves as Vice President of EFF-Austin, CLE Program Coordinator for SXSW, a leadership member of the Computer & Technology Section of the State Bar, a leadership member of Texas Exes Young Alumni- Austin, and the Founder of the Journal of Law and Technology at Texas. His practice focuses on startup and small business issues, and he provides subscription services for his clients. You can find out more about him and how he uses his CS background to inform his practice at shahrestanilaw.com.

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

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



Step 1
Go to Texasbar.com and click on "My Bar Page"

Step 2
Login using your bar number and password
(this will be the same information you'll use to login to the Section website)

If you see "Computer and Technology", congratulations, you're already a member.

If not, click the "Purchase Sections" button and follow the instructions to add the Computer and Technology Section. **Please note: It may take several days for the State Bar to process your section membership and update our system.**

You can also complete this form and mail or fax it in.

State Bar of Texas Computer & Technology Section Council

Officers:
John Browning – Dallas – Chair
Shawn Tuma – Plano – Chair-Elect
Elizabeth Rogers – Austin – Treasurer
Pierre Grosdidier – Houston – Secretary
Sammy Ford IV – Houston – Past Chair

Webmaster:
Judge Xavier Rodriguez – San Antonio

Circuits Editor:
Sanjeev Kumar – Austin

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

Term Expiring 2020:
Lisa Angelo – Houston
Eddie Block – Austin
Kristen Knauf – Dallas
Rick Robertson – Plano

Chairs of the Computer & Technology Section

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