COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas
March 2019

CLICK ON TITLE TO JUMP TO ARTICLE

Contents

Featured Articles:-

Short Circuits:-

CircuitBoard:-

Note from the Chair

By Sammy Ford

It is my pleasure to present the third issue of Circuits for the 2018-2019 Bar Year. In an effort to increase member services, we now publish the Section's newsletter quarterly. This increased publication schedule means that our members learn even more about the developments at the intersection of technology and the legal practice even more quickly.

On that note, on February 26, 2019 the Texas Supreme Court amended the Comment to Texas Disciplinary Rule of Professional Conduct 1.01. Texas joins 36 other states to adopt a comment specifying that remaining proficient and competent in the practice of law, requires staying abreast the "benefits and risks associated with relevant technology."

We were fortunate that this development occurred shortly before publication, and we could alert Circuit subscribers. Developments happen frequently, however. And I would, therefore, like to encourage Section members to join and participate in our mailing list discussion forum. The forum is moderated by the State Bar and allows members to get real time answers to their technology questions. You can subscribe to the mailing list at http://connect.texasbar.com.

I am also excited about our participation in two upcoming legal technology conferences around the country. First, two of our members will attend the ABA Techshow at the end of this month. They have promised to report back on the knowledge and experience gained at the conference; keep an eye out in these pages and on the website. Second, many of our members have been asked to present at the Louisiana Bar Association's Annual Technology conference. It is my hope that this participation will begin a process of collaboration between our respective bars on technology issues.

COMPUTER AND TECHNOLOGY SECTION

Letter from the Co-Editors

By Pierre Grosdidier & Kristen Knauf

Welcome to the third issue of *Circuits* for the 2018-19 bar year! In our last issue, we introduced a new section to our eJournal called *Short Circuits*, which provides short updates on recent developments in the case law or legislation. In this issue, we introduce another new section, called *CircuitBoard*. This section will feature articles of a technical nature on a topic of interest to attorneys. Readers will find no erudite case law and no beloved statutes in *CircuitBoard* but, technical expertise that will help them become better lawyers in our digital age (the *digitocene*?). Craig Ball and Ron Chichester, both past Section Chairs, stepped up to be our first *CircuitBoard* contributors (warning: if you lend Craig your iPhone, he will tell you where you have been within ten meters since the moment you first switched on the device).

We open this issue's Feature Articles with a contribution from Dan Shefet, the Danish-born French attorney who won a precedent-setting right-to-be-forgotten case against Google. It is an honor and a pleasure to host him as a guest author in *Circuits*. Dan summarizes recent privacy decisions from the European Court of Justice ("ECJ") on the Right to be Forgotten and extraterritoriality, and from the French Data Protection Agency, the *Commission nationale de l'informatique et des libertés*, regarding the €50 million Google fine.

Next, we are thankful to Judge Emily Miskel (current Section Council Member) to take the time to update us on the wrongful disclosure of video tape rental or sale records, a violation of the Video Privacy Protection Act ("VPPA," 18 U.S.C. § 2710). As Judge Miskel describes it, the VPPA is "an often-overlooked but very powerful [privacy] statute."

In the same vein as GDPR, but much closer to home, Ron Chichester (past Section Chair) gives us a comprehensive overview of the newly-enacted California Consumer Privacy Act of 2018. This new privacy law might be a harbinger of statutes to come in other states.

Cyber-attacks are all the rage these days, and attorneys are not immune. Lisa Angelo (current Section Council Member) updates us on ABA Ethics Opinion 483, which describes lawyers' ethical obligations after an electronic data breach or cyberattack. In this domain, issues both technical and legal can quickly get complicated. Shawn Tuma (current Section Treasurer) explains why companies (and, by implication, law firms) need to consult with an experienced cyber attorney.

If you thought that authorities needed a warrant to secure your cell-site location information ("CSLI") based on what you heard of *Carpenter v. United States*, think again. Yours truly (Pierre, current Section Webmaster and Circuits Co-Editor and former Section Council Member) reports on *Sims v. State*, a Texas court of appeals case that held that no warrant is required if the police pings a cell phone just a couple of times to track down a fliting fugitive.

Stephen Viña introduces us to cryptojacking. Cryptothugs spring from dark Internet alleys and snatch your computing power to mine cryptocurrency. If your computer is running slower than usual, it might have been cryptojacked. It is not reassuring news if you are operating a refinery or a nuclear power plant with a digital control system. Even driving on the Interstate might one day get hazardous. How soon before cryptocrooks capture the CPU of a fully-automated Interstate-cruising 18-wheeler and—its CPU busy churning and not driving—cause it to veer into a very real highway overpass pier?

Finally, William Smith explores what can happen when you post your DNA on 23andMe or on Ancestry. We all know how they caught the Golden State Killer. But, he is just the first of many. The *New York Times* ran a story on February 17, 2019, about another arrest related to an unsolved murder from 1993. William explains how these public DNA databases raise a slew of legal (and ethical) questions that presently have very few answers. These questions are important considering what is at stake. According to the *Times* article, "in the coming years, 90 percent of Americans of European descent will be identifiable, even if they have not submitted their own DNA." This news should bring solace to surviving relatives of otherwise long-forgotten crime victims (for whom evidence remains on dusty cold-case shelves) and, conversely, make living closet-skeleton-hiders mighty nervous. Also; memo to future violent criminals: hiding might no longer be an option.

In this issue's *Short Circuits*, John Browning (current Section Chair-Elect) summarizes the hullabaloo regarding the FaceTime bug; Ron Chichester introduces us to the upcoming EU's Privacy eDirective; Ryan Gardner (guest author) explains why the Information Quality Act (44 U.S.C. § 3516 note) is not the sword in the stone that will slay the administration's alleged misinformation; your truly (Pierre) reports on a privacy win (*In re Sun Coast*) regarding personal phone use at work; and Sanjeev Kumar (current Section Council Member) reports on Texas's plan to comply with the Federal REAL ID Act.

Many thanks to all the contributors to this new issue and for helping us keep this publication on schedule. Thank you also to Antony P. Ng for his review of and assistance with this issue's articles. We hope that you enjoy this new edition of *Circuits*, including *CircuitBoard*, and, as

always, we welcome any comments or submissions that you may have: please send them to our section administrator at admin@sbot.org.

Kind Regards,

Pierre Grosdidier, Co-Editor

Kristen Knauf, Co-Editor

Recent Important Decisions in Europe on "Global Reach" and Fines for Violations of the GDPR

By Dan Shefet

The first six weeks of 2019 have been rich in news from the European Court of Justice ("ECJ") on the Right to be Forgotten and extraterritoriality, as well as from the French Data Protection Agency ("DPA"), the *Commission nationale de l'informatique et des libertés* ("CNIL"),[1] on the consent requirements under the General Data Protection Regulation ("GDPR"). These developments augur increased judicial activity for the rest of the year not only on digital privacy, but also on Internet content moderation and accountability in general. United States attorneys specialized in European data privacy issues should closely monitor these developments.

Google Inc. v. CNIL (Case C 517/17)

On January 10, the Polish Advocate General of the ECJ, M. Maciej Szpunar, rendered his long-awaited opinion on the law and the facts in the matter of *Google Inc. v. CNIL*.[2] This is the first case at the ECJ level dealing with the territorial reach of European content and privacy regulations. The Advocate General declined to grant the CNIL's world-wide dereferencing request and instead offered a compromise solution circumscribed to the EU.

The CNIL fined Google €100,000 for its failure (*i.e.*, refusal) to dereference URLs from their search engine results when accessed from outside the EU and in particular on *google.com*. One of the CNIL's main arguments was that, in the name of effectiveness,[3] it was critical that delisting orders apply worldwide. Google and the various intervening parties (including Wikimedia Foundation Inc., *Fondation pour la liberté de la presse*, Microsoft Corp., the NGO

---

[1] The CNIL (pronounced "k-neel," *i.e.*, both the "k" and the "n" are pronounced) is an independent French administrative agency responsible for ensuring that computers (*informatique*, in French; the term is broader than computers and refers to all things digital) are not used to the prejudice of human rights, privacy, and liberties.

[2] Case C-507/17, *Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)*, 2019. The opinion is in French. An English-language press release is available here.

[3] *See* Article 19 of the Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community (2007/C 306/01) ("Member States shall provide remedies sufficient to ensure *effective legal protection* in the fields covered by Union law") (emphasis added).

Article 19, and others) argued that the EU and its member state Data Protection Agencies and judiciary did not have authority under international law to enforce their decisions outside of the EU.

This clash of laws and judgements is probably the most challenging legal problem facing the Internet today. The case is the first such dispute brought before a supranational court in an attempt to define territoriality and jurisdiction in "Cyberspace." It is a reminder of the work of the 17th century Jurist Hugo Grotius, who elaborated a set of laws applicable on the High Seas,[4] which still forms the basis for the leading international case on enforcement territoriality (*e.g.*, the *Lotus* case).[5] Cyberspace is in many respects akin to the High Seas and charting the international rules of navigation in this space is the daunting legal challenge put to the ECJ.

Typically, "territoriality" is divided into the legislative and adjudicatory rights of the sovereign state as recognized by the UN Charter.[6] Apart from certain human rights exceptions and intervention with Security Council clearance there is no real debate as to the right of states to legislate and adjudicate within their physical boundaries.[7] The thorny difficulty relates to enforcement rights outside of those physical boundaries or the international jurisdiction of the state (including occupied territories). The particular question put to the ECJ by the French *Conseil d'État* (the highest French administrative court, acting for the CNIL) pursuant to Google's challenge of the CNIL's global dereferencing order was essentially whether the CNIL had the right to enforce upon Google an obligation to take down links to searches made on non-European search engines (in this case on *google.com*) when accessed outside of EU.

From a pure public international law point of view, the principle of comity applies so that extraterritorial enforcement of laws and judgements depend on reciprocity. On this point it is worthwhile recalling US enforcement of certain laws worldwide. We see such enforcement for instance regarding discovery, money laundering, FCPA, Iran boycott, export regulations, antitrust and most recently, the U.S. Cloud Act (even if extraterritorial reach is met with hesitation by the U.S. Supreme Court).

The problem with the comity (or reciprocity) in this case is that of mutual recognition of "core values," *i.e.*, constitutional values *(e.g.*, the U.S. First Amendment). Because these values do not

---

4 H. Grotius, *Mare Liberum*, 1609. ("The Freedom of the Seas.")

5 *The case of the S.S. Lotus* (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).

6 Charter of the United Nations and Statute of the International Court of Justice (1945), San Francisco, United States.

7 U.N. Charter Art. 2, para. 1.

necessarily enjoy the same protection in all countries, the necessary level of reciprocity may not be attained. This problem arose in the Canadian *Google Inc. v. Equustek Solutions Inc.* case, where the Canadian Supreme Court affirmed a trial court decision ordering Google to delist Datalink search results worldwide.[8] The District Court for the Northern District of California held that the order was unenforceable and granted Google's request for injunctive relief.[9] But, even in *Equustek*, where the argument did not relate to free speech or similar "core values," but to intellectual property rights—which are recognized in both the US and Canada—the principle of comity was not applied. Google, to this day, has refused to comply with the global order rendered by the Canadian Supreme Court.

In *Google Inc. v. CNIL*, the Advocate General proposed a compromise solution that tracked, to a certain extent, Google's proposal: content and privacy orders should be delimited in territorial scope by an accessibility criterion. Under this solution, search engine results accessible from within the EU will not include links to the impugned URLs, while search engine results made against the same search criteria from outside the EU would be unrestricted. This rule would include searches made on *google.com*.

This solution implies the deployment of Internet Protocol ("IP") geo-localization features that are already broadly used, for instance, for copyright purposes (by commercial movie streaming sites, for example). Even though such location technology may be circumvented by virtual private network ("VPN") or similar technology, it will in the vast majority of cases suffice and satisfy an "efficiency" objective.

Apart from the fact that the legality of geo-localization is a moot question under the so-called "Digital Agenda"[10] and considering certain derogations allowed in favor of the European motion picture industry, it may well be that the European Court of Justice will follow the Advocate General's opinion because it opens up for global reach exemptions under certain circumstances. Unfortunately, the opinion does not provide examples of such exceptional circumstances, but describes them as arising in situations where the "interests of the Union necessarily require application of EU law outside of its territory. . . ."[11] Given that the GDPR (and the Directive 1995/46 before it) does not apply to "activities concerning national

---

[8] *Google Inc. v. Equustek Solutions Inc.*, [2017] 1 S.C.R. 34 (Can.).

[9] *Google LLC v. Equustek Solutions Inc.*, No. 5:17-cv-04207, 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017).

[10] A plan to create a single EU Digital Market is arguably incompatible with the compartmentalization of the EU.

[11] Case C-507/17, *Google Inc. v. CNIL*, at ¶ 62.

security,"[12] the exceptional circumstances must render extraterritorial application necessary in order to ensure efficient protection of privacy rights affecting data subjects within the EU territory. It is likely that such exceptions would also only be allowed in the event they are largely "core value neutral."

The ECJ's judgement in this case is expected in a few months. The Advocate General's opinion is not binding and, even though it is very often followed by the ECJ, it was not followed by ECJ in the famous case on the Right to be Forgotten.[13]

Right to be Forgotten update

On the same day (10 January) the Advocate General also rendered his opinion on the obligations of search engines to perform "systematic dereferencing" upon receipt of a request under the Right to be Forgotten (now codified in the GDPR's Article 17).[14] Even though this case may appear less important than the territoriality dispute discussed above, it is essential to the future enforcement of reputational and privacy rights in the European Union. The Advocate General recommended a systematic dereferencing obligation for sensitive data but allowed striking the balance between free speech as expressed under the so-called "journalistic exemption"[15] and privacy rights for non-sensitive data. A judgement in this case is also expected in a few months.

CNIL fines Google €50 million

On January 21, the CNIL handed down its decision to fine Google LLC €50 million. This is the first fine levied on the basis of the GDPR, which allows fines of up to 4% of global turnover. The decision is a direct application of the GDPR's articles 6, 12, and 13 relative to informed and transparent consent when configuring an Android phone and associated accounts. Google's alleged infringement was based in the complexity of user configuration and the lack of transparency (from users' perspective, and for each of the applications concerned) regarding the kind of data being collected, for what purpose, for how long it was retained, and whether it was transferred to third parties.

---

[12] General Data Protection Regulation, Recital 16 and Art. 2.2(a).

[13] Case C-131/12, *Google Spain SL v Agencia Española de Protección de Datos (AEPD)*, 2014.

[14] Case C-136/17, *G. C., A. F., B. H., E. D. v Commission nationale de l'informatique et des libertés (CNIL)*, 2019. The opinion is in French. An English-language press release is available here.

[15] General Data Protection Regulation, Article 85.2 (2016).

The CNIL announced that this was the first time that it assessed a monetary fine based on the GDPR.[16] It justified the amount of the fine based on the seriousness of Google's shortcomings regarding "essential principles of GDPR," namely, transparency, communication, and consent. Other factors included the amount of personal data involved, the fact that the offence was on-going (as opposed to a one-time lapse), and the large number of persons affected considering Android's "preponderant place" on the French smart device market.

Google has already announced its decision to challenge the fine before the *Conseil d'État*. But, it is highly doubtful that the *Conseil d'État* will overturn or reduce the fine because the CNIL's basis for its decision is a direct application of the GDPR's language and especially since—contrary to what seems to be one of Google's arguments—the decision will not ripple to small companies given that it makes direct reference to the "massive and intrusive" nature of the violations and the associated financial rewards (the latter reference is implicit).

GDPR journalistic exemption

Finally, on February 14, the ECJ handed down its decision in *Sergejs Buivids v. Data valsts inspekcija*[17] on the concrete application of the "journalistic exemption" found in Directive 95/46/EC of the European Parliament, and now replaced by GDPR Article 85.2. This is an area of content moderation and privacy that will most probably be the subject of litigation for some years to come. In this case, Buivids, a Latvian citizen, video-recorded police officers and staff at a police station while he was making a statement, and later posted the video on YouTube. The individuals filmed claimed that this amounted to a violation of their privacy (their work place being "private" under the GDPR) and prevailed before the national DPA and courts. The ECJ, in response to certified questions from the Latvian Supreme Court (technically, a response to a pre-judicial question of interpretation), held that "the video recording of police officers in a police station, while a statement is being made, and the publication of that recorded video on a video website, on which users can send, watch and share videos, may constitute a processing of personal data *solely for journalistic purposes*."[18] In other words, Buivids' conduct might fall under the journalistic exception in Directive 95/46/EC. The ECJ thus confirmed its broad construction of the expression "journalistic activities" even though it left the final qualification to member state courts, as in this case. But, the ECJ promulgated an important criterion for use

---

[16] Press Release, Commission nationale de l'informatique et des libertés, *La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société GOOGLE LLC* (Jan. 21, 2019).

[17] Case C-345/17, *Sergejs Buivids v. Data valsts inspekcija*, 2019.

[18] *Id.* at ¶ 69 (emphasis added).

by member state courts: it is the intention of the author that is decisive. If that intention was exclusively "journalistic" the exemption might apply.

These developments show that data privacy issues will likely play a significant role in the ECJ's docket and the individual National Data Protection Agencies' priorities in 2019 and beyond.

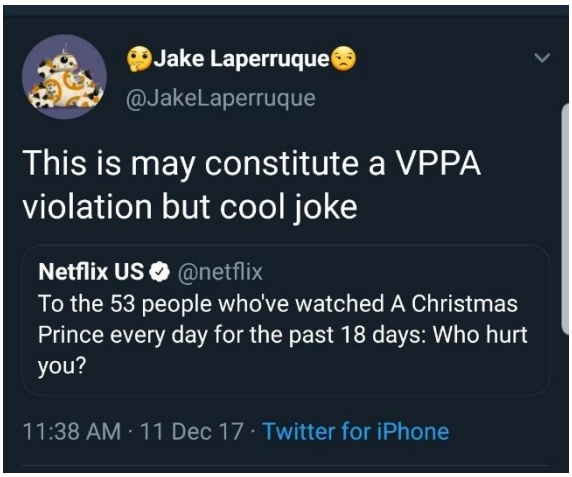
About the Author

Dan Shefet is an attorney in Paris France. He specializes in data privacy and information technology ("IT") Law, is an Individual Specialist to UNESCO, and an Expert with the Council of Europe. He obtained the first judgement enforcing daily penalties pursuant to the Right to be Forgotten on the Internet. Dan is a frequent speaker at international conferences on IT law, data privacy, and content regulation. In 2014, he founded the Association for Accountability and Internet Democracy (AAID), whose main objective is to introduce a general principle of accountability on Internet.

Somebody's Watching Me Recent Updates on the Video Privacy Protection Act

By Judge Emily Miskel

I first learned of the Video Privacy Protection Act (VPPA) when Netflix tweeted:



"To the 53 people who've watched A Christmas Prince every day for the past 18 days: Who hurt you?"

and user @JakeLaperruque responded "This may constitute a VPPA violation but cool joke."

I found the VPPA in 18 U.S. Code Chapter 121, along with the Stored Communications Act.[1] This law prohibits a "video tape service provider" from disclosing personally identifiable information about consumers. The civil action in the Act allows liquidated damages of $2,500, actual damages, punitive damages, attorney fees, and equitable relief. It also contains a strong exclusionary rule, providing that wrongfully-obtained Personally Identifiable Information (PII) may not be evidence in any government proceeding.

History

The reference to video *tapes* is a clue that this law has been on the books for a while. The law was originally passed in 1988 in response to a newspaper's printing of Supreme Court nominee Robert Bork's video rental records. It was amended in 2011 with the support of new entertainment companies, like Netflix, whose business models rely on monetizing consumer information.

Although the act refers to "tapes," the definitions extend VPPA protections to new forms of streaming media and rental services like Redbox. Under the Act, a "video tape service provider" is someone in the business of rental, sale, or delivery of prerecorded video cassette tapes or *similar audio-visual materials*.

[1] 18 U.S. Code 2710, "Wrongful disclosure of video tape rental or sale records."

Consent

When passed, the VPPA contained one of the strongest statutory user-consent provisions available. In its original form, the VPPA required consumer consent to be given at the time a disclosure of personally identifiable information (PII) was sought.

Several class action lawsuits were filed in 2011 against Netflix for violating the VPPA.[2] Under the VPPA, video rental companies must destroy PII as soon as practicable but no later than one year after the information is no longer necessary for its collected purpose.[3] The suits alleged that the companies indefinitely retained PII and provided it to third parties without consent. The law was amended in 2011, and the suits settled.

The 2011 amendments allowed companies to obtain the user's consent up to 2 years in advance, but also required that the consumer have the ability to withdraw consent on a case-by-case or ongoing basis. This amendment enabled companies like Netflix to share consumer information with companies like Facebook, for example, by obtaining user consent in their terms of service.

What counts as PII?

In 2016, the 1st Circuit held that unique data markers may identify a person for the purposes of the VPPA, even if the user's name is not disclosed.[4] Although the USA Today mobile app did not obtain user consent to disclose information, each time the user viewed a video, the app sent to Adobe the title of the video, the GPS coordinates of the device at the time of viewing, and unique device identifiers. Adobe offered data analytics, and the unique device IDs allowed Adobe to track users across platforms. The 1st Circuit clarified that a person may still be identifiable by PII through GPS or device identifiers even if the person's name is not disclosed.

That same year, the 3rd Circuit articulated a different test for whether information was capable of identifying a person under the VPPA.[5] The *Nickelodeon* case held that the Act's prohibition on the disclosure of PII applied only to the kind of information that would readily permit an *ordinary person* to identify a specific individual's video-watching behavior. The court held that digital identifiers like IP addresses fell outside the Act's protections.

---

[2] *See, e.g.*, *Milans v. Netflix, Inc.*, Case No. 5:11-cv-00379 (N.D. Cal. filed Jan. 26, 2011); *Missaghi v. Blockbuster, LLC*, Civil No. 11-2559 (D. Minn. filed Sep. 6, 2011).

[3] 18 U.S. Code 2710(e).

[4] *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 486 (1st Cir. 2016).

[5] *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 284 (3d Cir. 2016).

In 2017, the 9th Circuit also adopted the "ordinary person" test.[6] The court found that the "ordinary person" test better informed video service providers of their obligations under the VPPA, by focusing on what information a video service provider "knowingly discloses." The court declined to hold the discloser responsible for the ways the recipient of the information could use technology to identify users.

Who is a consumer?

The VPPA protects "consumers," including any renter, purchaser, or subscriber of goods or services from a video tape service provider. There is currently a circuit split on whether users of free apps can be considered consumers/subscribers under the VPPA.

The 11th Circuit held in 2015 that a user's downloading and using a free app from the Cartoon Network did not make him a subscriber under the VPPA.[7] The court concluded that a subscription involves commitment, whether that be payment, registration, access to restricted content, or other relationship between the person and the entity.

However, the 1st Circuit held in 2016 that a person who viewed content through a proprietary USA Today news app could be a consumer or subscriber, even if he did not pay for a service.[8] The court held that the user was a subscriber because the user provided personal information in return for the video content and downloaded the app rather than merely viewing a website.

New Issues – Smart TVs

A new frontier for VPPA litigation is in the realm of smart televisions. Smart TVs provide apps and enhanced content, but also monitor users' viewing habits and sell that information to third parties. Smart TVs capture pixels that identify the program being watched. They send that data back to the manufacturer, along with other data including the IP address, MAC address, wifi network information, and more. The manufacturer sells the data to third parties who combine it with other sources to determine demographic information about the customer's household.

Vizio, one maker of smart TVs is the subject of a pending class-action VPPA lawsuit. The 9th Circuit denied a motion to dismiss, finding that Vizio was engaged in the business of delivery of video content and that users are consumers because they have paid a premium price for the

---

[6] *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 984-86 (9th Cir. 2017)

[7] *Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251 (11th Cir. 2015).

[8] *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 487-88 (1st Cir. 2016).

smart TV.[9] The court further applied the *Yershov* test and concluded that the information disclosed, including:

> MAC addresses, IP addresses, zip codes, chipset IDs, product model numbers, hardware and software versions, region and language settings, viewing history, purchase history, and the presence of other devices connected to the same network,

was PII.

In contrast, a class-action smart-TV lawsuit in New Jersey was recently dismissed, because under the "ordinary person" test followed by the 1st and 3rd circuits, the information collected and disclosed by the smart TVs was not considered PII.[10]

Conclusion

The VPPA is an often-overlooked but very powerful statute. Anyone engaged in delivering video content should be aware of its provisions. And of course, consumers should be knowledgeable about all of the personally-identifiable information that is being tracked and sold by video content deliverers.

About the Author

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

[9] *In re Vizio, Inc., Consumer Privacy Litigation*, 238 F.Supp.3d 1204 (C.D. Cal. 2017).

[10] *White v. Samsung Electronics America, Inc., et al.*, No. 17-1775 (D.N.J. Sept. 26, 2018).

The California Consumer Privacy Act of 2018: GDPR Hits Close to Home

By Ronald Chichester

The California Consumer Privacy Act of 2018[1] ("CCPA") is a new form of privacy initiative that borrows from Europe's GDPR.[2] While the CCPA's penalties are not as severe as GDPR's,[3] the chances of encountering CCPA-entanglements are more likely for Texas companies. Moreover, CCPA is setting a trend that was started by GDPR, and more states may adopt CCPA-like statutes.

I. Some History About the Act

The CCPA had a very quick gestation. Indeed, the law was passed within a frantic seven-day legislative initiative that was clearly designed to thwart a possibly more draconian ballot initiative that was started by Alastair Mactaggart in 2017. That ballot initiative drew widespread industry condemnation and a $100M+ campaign to stop it. This short gestation period for CCPA is in stark contrast to the four-year gestation period for GDPR. Such haste led to the passage of the CCPA on June 28, 2018, and the passage of its first amendment (Senate Bill 1121[4]) on September 23, 2019. The CCPA does not take effect until January 1, 2020, so additional amendments are not out of the question, although *substantive* amendments are not deemed likely lest the ballot initiative be reinstated.

II. In General

The CCPA can be categorized as an opt-out (for adults, but opt-in for minors) privacy act that covers a broad range of information about California-located consumer transactions involving California residents. The CCPA has several GDPR-like provisions that are of interest to Texas businesses. In general, consumers have certain (limited) rights, and businesses have certain (limited) duties. While the CCPA has had its share of fear/hype, the provisions within CCPA have several major loopholes, so businesses may not have as much to fear as the media hype suggests.

---

[1] TITLE 1.81.5. California Consumer Privacy Act of 2018 (§§1798.100-1798.199).

[2] General Data Privacy Regulation, (EU) 2016/679.

[3] *See* Eric Goldman, *A Privacy Bomb Is About to Be Dropped on the California Economy and the Global Internet*, Technology and Marketing Law Blog, June 27, 2018.

[4] *See* California Senate Bill 1121.

The CCPA provides: a right to disclosure (for the consumer);[5] a right to delete (for the consumer);[6] delineates what businesses must disclose;[7] duties imposed on covered businesses;[8] opt-out provisions for adult consumers and opt-in requirements for minors;[9] prohibition on discrimination of consumers (by a business) for exercising their rights under the CCPA;[10] the form of a request for disclosure;[11] additional duties on businesses related to opt-out;[12] a set of definitions; [13] some limitations on the duties of businesses;[14] violations/rights of action/remedies;[15] the right to seek the opinion of the Attorney General;[16] a consumer privacy fund (to compensate the state);[17] reference to other privacy laws;[18] preemption of other state and local rules and regulations;[19] requirements of the Attorney General;[20] an anti-circumvention provision;[21] no-waiver of CCPA provisions by contract;[22] a plea for liberal construction of the law;[23] a limitation on preemption;[24] the date of enforceability (January 1, 2020);[25] and early operability of the date of enforceability and limited preemption provisions (September 23, 2018).[26]

---

[5] CCPA §1798.100.
[6] CCPA §1798.105.
[7] CCPA §1798.110.
[8] CCPA §1798.115.
[9] CCPA §1798.120.
[10] CCPA §1798.125.
[11] CCPA §1798.130.
[12] CCPA §1798.135.
[13] CCPA §1798.140.
[14] CCPA §1798.145.
[15] CCPA §1798.150.
[16] CCPA §1798.155.
[17] CCPA §1798.160.
[18] CCPA §1798.175.
[19] CCPA §1798.180.
[20] CCPA §1798.185.
[21] CCPA §1798.190.
[22] CCPA §1798.192.
[23] CCPA §1798.194.
[24] CCPA §1798.196.
[25] CCPA §1798.198.
[26] CCPA §1798.199.

III. Covered Transactions

The CCPA only covers certain data-capturing transactions that occur in California that concern California residents. Well, a savvy lawyer might opine that a way around that restriction would be to record the data while in California, but only upload that data *after* the consumer has left the state. Not so fast. The CCPA anticipated such an attempt at circumvention, and prohibited it.[27]

IV. Businesses Covered

The CCPA defines a "business" broadly, but the law is directed to for-profit entities that do business in California.[28] However, in order to be a "covered business" under the CCPA, a for-profit business entity must also satisfy one of the following "thresholds":

1. Has annual gross revenues in excess of twenty-five million dollars ($25,000,000)
2. Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or
3. Derives 50 percent or more of its annual revenues from selling consumers' personal information.

These thresholds exclude many small businesses. The second threshold, however, begs a question: was that 50,000 *California* consumers, or just consumers in general? The CCPA defines "consumer" as "a natural person who is a *California* resident."[29] How businesses are supposed to track whether a consumer is a California resident (or not) can be difficult, but the effort may be worthwhile for businesses on the cusp of the threshold. Large corporations that focus on consumer surveillance (regardless of where they are located) are obviously affected—indeed they were the intended targets of the Act.

---

[27] *See* CCPA §1798.190 ("If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.").

[28] *See* CCPA §1798.140(c)(1).

[29] *See* CCPA §1798.140(g).

V. Disclosure Requirements

California residents have the right to request that a covered business disclose the categories and specific pieces of personal information collected.[30] The disclosure must occur at the time of, or *before*, the transaction takes place. Interestingly, exactly *what* gets disclosed differs depending on whether the business has *sold* the personal information or merely *disclosed* the personal information to a third party. The covered business may disclose (as part of its privacy policy) or otherwise be required to disclose the following:

- If the business has ***sold*** personal information about consumers, then the business must provide a list of categories of personal information that it has sold about consumers in the preceding twelve months that most closely describe the information that was sold;
- If the business has **not** sold personal information, that fact must be disclosed;
- If the business has disclosed (but not sold) personal information about consumers, then the business must provide a list of the categories of personal information that it has

---

[30] *See* CCPA §1798.100(a). CCPA §1798.140(o)(2) excludes publicly available information. However, CCPA §1798.140(o)(1) defines personal information broadly to include "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

A. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
B. Any categories of personal information described in subdivision (e) of Section 1798.80.
C. Characteristics of protected classifications under California or federal law.
D. Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
E. Biometric information.
F. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.
G. Geolocation data.
H. Audio, electronic, visual, thermal, olfactory, or similar information.
I. Professional or employment-related information.
J. Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).
K. Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

disclosed for a business purpose in the preceding twelve months that most closely describe the personal information disclosed;

- If the business has ***not*** disclosed personal information about consumers, then that fact must be disclosed;
- The specific pieces of personal information that the business has already collected from the consumer;
- The categories of sources from which the personal information is collected;
- The business or commercial purpose for collecting or selling or disclosing personal information; and
- The categories of third parties with whom the business shares personal information.[31]

By using "categories," covered businesses are relieved from telling consumers the actual identity of the third parties that receive their personal information. Unfortunately, this loophole makes it difficult (if not impossible) for California consumers to request the third parties to delete their data—which defeats the purpose of the CCPA. In any case, an obvious way to satisfy the disclosure requirement would be to post a notice at the retail establishment (preferably near the point of sale), or on the company's website. However, the California Attorney General will likely be asked to opine as to suitable disclosure mechanisms.

One of the key phrases in the CCPA is "a verifiable consumer request." This important definition is covered in §1798.140(y).[32] One of the loopholes in the Act is that businesses are not required to disclose data or delete data if they cannot verify the identity of the consumer making the request. Presumably the verification process should not be onerous, but it may require effort on the part of the consumer, and that might be enough to nullify the effect of the law for many consumers—particularly if they have to go through the process with many businesses. Moreover, consumers can only obtain such a disclosure at most twice in a 12-

---

[31] *See* CCPA §1798.100(b) and §1798.110 for a full list of the disclosure requirements.

[32] "'Verifiable consumer request' means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf."

month period. Importantly, the information used to verify the request can be used only for the purpose of verification.[33]

Once the verified customer request has been received, the covered business must deliver the information promptly—and free of charge.[34] Delivery can be made electronically or by mail. If made electronically, the information must be in a form that can be copied or forwarded easily by the consumer (*i.e.*, no digital rights management or other mechanisms to prevent printing, copying or forwarding of the disclosed information).[35] Businesses have 45 days from the receipt of the verifiable consumer request to disclose the information.[36]

One foolproof mechanism for eliminating the disclosure requirement is simply not to collect personal information about the consumer. The CCPA does not require businesses to retain any personal information for a single, one-time transaction, if that information is not sold or retained by the business to re-identify or otherwise link information "that is not maintained in a manner that would be considered personal information."[37] Aggregated information (that does not identify a customer) is similarly excluded.[38]

Finally, the business must have disclosures on an online privacy policy (if it has one) or on a California-specific description of rights within the company's website.

VI. Right to Opt-Out

Consumers have a right to opt-out of the sale of their personal information.[39] Once the consumer has opted-out, the covered business is prohibited from selling that consumer's personal information from that point forward—unless the covered business obtains an express authorization from the consumer for the sale.[40] While businesses may *ask* the consumer for

---

[33] CCPA §1798.130(a)(7).

[34] CCPA §1798.100(d). However, if the requests are manifestly unfounded or excessive (by repetition), the business is allowed to charge a reasonable fee for those requests. *See* CCPA §1798.130(g)(3).

[35] *See* CCPA §1798.100(d).

[36] CCPA §1798.130(a)(2). Note, this deadline refers to the date when the verifiable consumer request was received, not when the request was actually verified. Verification is optional. The business may obtain a 45-day extension if it notifies the consumer of the extension. *Id.* Interestingly, CCPA §1798.145(g)(1) says that the second period is 90 days (not 45) if the business informs the customer within the first 45 days with an explanation for the delay. Presumably this discrepancy will be resolved before the law is enforced.

[37] CCPA §1798.100(e) and §1798.110(d).

[38] CCPA §1798.140(o)(2).

[39] *See, in general,* CCPA §1798.120 and §1798.135.

[40] CCPA §1798.120(c).

permission to sell their personal information, they may do so only after a 12-month period has expired.[41] Interestingly, consumers may use a *proxy* to exercise their opt-out rights.[42] Businesses may rightly fear the creation of for-purpose proxies to relieve consumers of the tedious chore of opting-out of sales of their personal information. In any event, businesses are encouraged to provide clear and conspicuous links on their websites entitled "Do Not Sell My Personal Information" that facilitates the exercise of the consumer's right to opt-out of the sale of their personal information.[43]

Finally, there is a general prohibition of selling personal information about children under the age of 16.[44] However, if the minor is between 13 and 16, they (themselves) may opt-in.[45] For children under 13, their parent or guardian must provide affirmative authorization.[46]

VII. Right to Delete

Upon receipt of a verifiable consumer request to delete the consumer's personal information, a covered business "shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records."[47] Moreover, covered businesses must *inform* consumers of their right to have their personal information deleted.[48] This may prompt companies to sell the personal information as quickly as possible—before consumers have a chance to say, "delete."

There are several caveats to the deletion requirement. Businesses are not required to comply with a deletion request if:

1. The personal information is needed to complete a transaction that was requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise to perform a contract between the business and the consumer.[49]

---

[41] CCPA §1798.135(a)(5).
[42] CCPA §1798.135(c).
[43] CCPA §1798.135(a)(1).
[44] CCPA §1798.120(d).
[45] CCPA §1798.120(c).
[46] *Id.*
[47] CCPA §1798.105(c).
[48] CCPA §1798.105(b).
[49] CCPA §1798.105(d)(1).

2. The information is needed to detect fraud, malicious, or illegal activity (or prosecute those responsible for the bad acts).[50]
3. Detect and fix bugs in software and related-systems.[51]
4. Exercise free speech; ensure the right of another consumer to exercise his or her right to free speech; or exercise another right provided for by law.[52]
5. To comply with the California Electronic Communications Privacy Act.[53]
6. Engage in public or peer-reviewed research *if* the consumer has provided informed consent.[54]
7. To enable *solely internal uses* that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.[55]
8. To comply with a legal obligation.[56]

VIII. Obligation Not to Discriminate

Businesses are prohibited from discriminating against consumers who have exercised their rights under the CCPA.[57] There are several specific types of discrimination that are delineated in the CCPA, including:

- The denial of goods and services to the consumer by the business;
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits (or even by imposing penalties); or

---

[50] CCPA §1798.105(d)(2).

[51] CCPA §1798.105(d)(3).

[52] CCPA §1798.105(d)(4). Sadly, I am at a loss to know what this means. How is the act of ***not*** deleting someone's personal information somehow free speech? If the data is somehow used as an affirmative defense to defamation/libel, perhaps?

[53] CCPA §1798.105(d)(5), specifically pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the California Penal Code.

[54] CCPA §1798.105(d)(6).

[55] CCPA §1798.105(d)(7) and the closely aligned provision of §1798.105(d)(9). What is "reasonably aligned" and how do you discern "the consumer's relationship with the business"? Is it storing a credit card number (along with the consumer's name and address) so that the consumer can return to a website and purchase more product (assuming the consumer has checked some checkbox)? Hopefully the California Attorney General will shed some light on this within the first six months of enforcement of the Act.

[56] CCPA §1798.105(d)(8).

[57] *See generally*, CCPA §1798.125.

- Providing (or even *suggesting* that the business will provide) a different level of quality of the goods or services to the consumer when the consumer exercises his or her rights under the Act.

However, the provision about a price differential is not absolute. A business *may* charge a different price or rate *if* that difference is "reasonably related to the value provided to the consumer by the consumer's data."[58] Similarly, a "business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data."[59]

IX. Violations and Remedies

Businesses are liable for unauthorized disclosure of unencrypted or non-redacted personal information.[60] Consumers have the right to civil actions, including class actions.[61] Consumer must, however, provide the business with a 30-day notice, and the business has those 30 days to cure the violation and inform the customer of the specifics of that cure.[62] The civil actions under the CCPA cannot be combined with actions under other laws.[63]

X. What to Do

The obvious work-around would be to collect only as much information, and for only as long as necessary, to satisfy critical business functions, such as facilitating the transaction itself.

Ensure that employees are trained about the CCPA. Specifically, businesses are responsible for ensuring that all individuals (regardless of whether they are employees or contractors) who are responsible for handling consumer inquiries about the business's privacy practices or the

---

[58] CCPA §1798.125(a)(2).

[59] CCPA §1798.125(b)(1).

[60] CCPA §1798.150(a)(1). Damages, under a civil action, include recovery of $100 to $750 per customer per incident or actual damages (whichever is greater); injunctive or declaratory relief; and any other relief the court deems proper. CCPA §§1798.150(a)(1)(A)-(C).

[61] CCPA §1798.150(b).

[62] *Id.*

[63] CCPA §1798.150(c).

business's compliance with the CCPA understand all of the requirements and know how to inform consumers how to exercise their rights.[64]

XI. Conclusions

The CCPA was a rushed response to forestall a harsher sanction on businesses that routinely collect and sell consumers' personal information. Even though there are some internal inconsistencies in the Act, they will likely be ironed out before the law's enforcement. However, the sentiment and message is clear—California consumers will have some modicum of sovereignty over their personal information.[65] The penalties are individually modest, but collectively significant. The administrative overhead required by the Act, however, may make such data collection cost-prohibitive. Even though this law is limited to California, it may well be a template for other states and a harbinger of things to come. Clearly, there will be no more free lunches for the Marketing Department—***IF*** consumers actually exercise their rights to opt out and delete, which is by no means certain.

About the Author

Ronald Chichester is a solo practitioner in Tomball who specializes in technology-related legal issues. He is past chair of both the Business Law Section and the Computer & Technology Section. Ron is a former adjunct professor at the University of Houston where he taught courses in computer crime and e-commerce. He is a registered patent attorney, a certified computer forensics examiner and a certified information systems auditor. Ron received his JD from the University of Houston and he holds a bachelor's and a master's degree (both) in aerospace engineering from the University of Michigan.

[64] CCPA §1798.130(a)(6) and §1798.135(a)(3).

[65] This individual data sovereignty has been advocated by intellectuals such as Jaron Lanier in his book WHO OWNS THE FUTURE and other books.

ABA Ethics Opinion 483: A Data Breach Might Mean Ethical Violations for Lawyers

By Lisa M. Angelo

A law practice is like any other business in that it is susceptible to cyberattacks. Unlike most businesses, lawyers have very particular ethical obligations including the responsibilities to be competent, protect client information, and maintain confidentiality.[1] Cyberattacks can take many forms, but they typically aim to obtain information, steal money, or interrupt operations. A cyberattack that impacts a law practice might also cause a lawyer to violate ethical obligations and face legal liability.[2]

It is generally accepted that data breaches are inevitable. But if a data breach is inevitable, then must it also be inevitable that lawyers will violate their ethical obligations? Not necessarily… Whether a law practice's data breach means a lawyer has violated any ethical obligations depends on what steps that lawyer took before and after the breach.

Formal Opinion 483

The American Bar Association's Model Rules of Professional Conduct are baseline standards of legal ethics for lawyers. Although not binding, they are often adopted by the states. In the Fall of 2018, the ABA's Committee on Ethics and Professional Responsibility issued Formal Opinion 483 describing lawyers' ethical obligations after an electronic data breach or cyberattack.[3] Formal Opinion 483 will provide helpful guidance to lawyers preparing for and responding to a data breach. It is likely that states will also consult Opinion 483 for its definition of a data breach and description of how to apply already existing rules of ethics when a law practice is breached.

This article summarizes important issues discussed in Opinion 483 such as how a "data breach" is defined by the ABA compared to statutory definitions, and how lawyers might avoid violating existing rules of ethics after a breach.

---

[1] MODEL RULES OF PROF'L CONDUCT R. 1.1, 1.15, 1.6 (2018).

[2] ABA Comm. On Ethics & Prof'l Responsibility, Formal Op. 483 (2018) (Lawyers' Obligations After an Electronic Data Breach or Cyberattack).

[3] *See Id.*

How a Data Breach Might Lead to Ethical Violations

According to the Committee, an ethical violation occurs "when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach."[4]

To avoid an ethical violation after a data breach, a lawyer must understand which ethical obligations are triggered and which actions are reasonable. The following factors are considered to determine compliance with the Model Rules of Professional Conduct: (1) the nature of the cyber incident; (2) the ability of the attorney to know facts and circumstances of the cyber incident; (3) the attorney's role at the firm; and (4) the attorney's level of authority at the firm.[5]

What is a Data Breach?

The phrase "data breach" is defined differently by various laws and jurisdictions. The ABA's Committee defines a "data breach" as

> a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.[6]

It is important to note that the Committee's definition of data breach is different from definitions in other jurisdictions. Under the Committee's definition of data breach, the type of data concerned is information related to the representation of a client, namely, material client confidential information.[7] Other data privacy laws are concerned with any data that could be used to identify an individual or otherwise known as "personally identifying information" (PII), regardless if it belongs to a client. Even though these definitions overlap, they are different. To determine the best course of action, lawyers must pay careful attention to which laws are triggered by a cyberattack.

How Data Privacy Laws Impact Lawyers

Another notable difference among definitions of "data breach" is that, typically, a breach can occur when relevant information is misappropriated, destroyed or otherwise compromised. The

---

4 *Id.* at 6.
5 *Id.* at 2.
6 *Id.* at 4.
7 *Id.* at 2 & 4.

Committee adds, "or where a lawyer's ability to perform the agreed scope of legal services is significantly impaired by the episode."[8]

A cyber incident that could limit a lawyer's ability to perform includes ransomware attacks that essentially lock the lawyer out of the firm's files. For example, the lock-out might prevent the lawyer from meeting a deadline, therefore limiting the lawyer's ability to perform legal services. It is possible that during the lock-out, no data is exposed. The Committee suggests that such a scenario is a data breach. However, under some data privacy laws, because no data is exposed, such a scenario is *not* a data breach.

The Committee acknowledges the differences among laws governing data breaches and reminds lawyers that many obligations may be triggered by a cyber incident. For example, many lawyers might be surprised to know that a cyber incident could subject a Texas lawyer to liability in another jurisdiction.[9] As a matter of best practice, the Committee encourages lawyers to conduct separate evaluations of data privacy laws and rules of ethics to ensure full compliance.[10] The Committee warns lawyers that despite any overlap, compliance with rules of ethics will not necessarily equal compliance with the other laws, and vice versa.[11] Like most matters involving data privacy, cross-jurisdictional and cross-sectoral compliance is imperative due to lack of uniformity among the laws.

New Technology, Same Ethics

Whether dealing with paper files or electronic data, the same underlying ethical obligations apply. Technology complicates things by creating many opportunities to access the data.

Consider how law firms have historically treated paper files. In the recent past, paper files may have been stored in a secured file room. Access to the room would have been restricted, and there may have been a process to check files in and out. If a file was missing, there may have been a method to track the file's location by retracing the history documented during check out. These precautions were necessary to comply with the rules of ethics such as the duty to maintain confidentiality.

Today, because most law firms store files electronically; a door leading to the file room is only one of many data access points.

---

[8] *Id*. at 4.

[9] State consumer data privacy and breach notification laws in other states can affect Texas attorneys.

[10] Formal Op. 483 at 2.

[11] *Id*. at 2.

In 2012, the ABA clarified that a lawyer's duty to maintain competence included understanding the benefits and risks of using technology.[12] On February 26, 2019, a similar amendment was adopted in Texas.[13] In Opinion 483, the Committee recaps several prior opinions on how technology impacts fundamental rules of ethics before diving into an explanation of how ethics apply to a data breach.

Avoid Ethical Violations

Even though a data breach might be inevitable, an ethical violation doesn't have to be. In its Opinion 483, the Committee describes a strategy lawyers can implement to properly address cyber incidents and prevent data breaches from resulting in ethical violations. The strategy includes steps to monitor, stop, restore, and assess damage.[14]

Monitor

How would you know if you were breached? Furthermore, because the Committee defined a data breach as involving material client confidential information, lawyers must have a method for identifying when such information has been exposed.

> [L]awyers must employ reasonable efforts to monitor the technology and office resources connected to the Internet, external data sources, and external vendors providing services related to data and the use of data.[15]

Not only should unauthorized activity be monitored on a lawyer's computer, but it should be monitored on all devices used to handle data. This includes mobile devices, printers, scanners, employees' devices, and external vendors (cloud services, practice management cloud services, e-fax, phone answering services, etc.) To adequately monitor the network, lawyers need to understand how the firm accesses, stores, and shares data before they can implement the

---

[12] MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. [8] (2018).

[13] TEX. DISCIPLINARY RULES OF PROF'L CONDUCT R. 1.01 cmt. [8] (2019) ("Because of the vital role of lawyers in the legal process, each lawyer should strive to become and remain proficient and competent in the practice of law, including the benefits and risks associated with relevant technology. To maintain the requisite knowledge and skill of a competent practitioner, a lawyer should engage in continuing study and education. If a system of peer review has been established, the lawyer should consider making use of it in appropriate circumstances. Isolated instances of faulty conduct or decision should be identified for purposes of additional study or instruction.")

[14] An example of a commonly referenced framework is *NIST Computer Security Incident Handling Guide* (2012).

[15] Formal Op. 483 at 5.

proper tools and processes. If a device connects to the firm's intranet, it probably needs to be monitored.

Stop & Restore

Once you successfully monitored the network and identified a data breach, you must take prompt action to stop the breach and restore the systems to mitigate damage and continue operating the firm.[16] After taking prompt action to stop the breach, lawyers must make all reasonable efforts to restore computer operations to service the needs of clients.[17]

Assess Damage

A post-breach investigation is necessary for a lawyer's further compliance with ethics rules. To comply with duties to maintain competence, a lawyer should learn the details of what happened during the breach and understand how to reduce chances of suffering from similar situations in the future.[18] A lawyer is also ethically obligated to keep clients reasonably informed about their legal matters. The information gathered in a post-breach investigation can help the lawyer understand the scope of the intrusion and what must be disclosed to the client. Lawyers should attempt to learn the following in a post-breach investigation:

1. Whether electronic files were accessed, and if so, which ones;"[19]
2. What occurred during the breach;
3. That the intrusion has been stopped; and
4. Evaluate the data lost or accessed.

Be Proactive

The Committee suggests that before ever suffering from a data breach, lawyers should be proactive and plan specific procedures to promptly respond to an incident. An incident response plan should be tailored to fit the firm's specific practice and processes.[20] Although not mandated by the rules of ethics, such a plan can help support a lawyer's claim that actions taken were reasonable.

---

[16] *Id*. at 6.
[17] *Id*. at 7.
[18] *Id.*
[19] *Id*.
[20] *Id*.

Where to Start (to Reduce Your Firm's Cyber Liability)

Technology-related matters can be complex and challenging for many lawyers to grasp, let alone maintain the requisite competence. Those struggling to understand cybersecurity may be relieved to know that a lawyer's competency can be satisfied by employing qualified lawyer and nonlawyer assistants.[21]

If lawyers want to survive in the practice of law, they must understand the costs and benefits of using technology. Lawyers must understand how to implement security and reasonably prepare and respond to a cyber incident. What you did not do *can* hurt you.

For help with managing data privacy and cybersecurity, I suggest reviewing the ABA and other state bar websites for guidance. Most bars offer tips on how to manage data privacy. Of course, Opinion 483 is a great place to start. You might also consider hiring a data privacy/cybersecurity lawyer to assist your firm.

About the Author

Lisa M. Angelo is an attorney focused on helping businesses mitigate and manage cyber liability. She advises clients on data privacy, cybersecurity, business transactions, and other areas related to cyber law. Lisa also has a strong background in insurance law and helps clients with cyber insurance disputes. Lisa is the founding attorney of a forward-thinking, "virtual" law practice. She is an elected council member for the State Bar of Texas Computer & Technology Section. She also serves as the Vice-Chair of the State Bar of Texas Business Law Section's General Practice Committee and is a member of the Blockchain Committee. In addition, she is a member of the FBI's InfraGard Houston Chapter. Lisa is a Certified Information Privacy Manager and licensed to practice law in Texas and Colorado. She earned a Juris Doctorate from South Texas College of Law and a bachelor's in psychology from The University of Texas at Austin.

[21] *Id*. at 4.

Why Your Company Needs an Experienced Cyber Attorney

By Shawn Tuma

In recent years, companies have begun to understand that cyber is an overall business risk, not just a technical issue. Now they must realize that cyber is also a legal issue. The easiest way to understand this concept is to ask the following two questions: "Why do we know about the data breaches of Target, Yahoo!, Equifax and all the others?", and "did those companies air their dirty laundry just because they believed it was the right thing to do?"

Of course not! They did so because laws and regulations made them. Those laws and regulations require companies to disclose their breaches and mandate things such as who they must notify, when and how they must notify, what must be communicated and what must be done for those who were impacted. As these rules demonstrate, having data creates risk and one of legal counsel's roles is to help companies manage that risk.

Many attorneys explain their primary value through their wielding of the attorney-client privilege, by helping to cloak the cyber risk management process with the attorney-client privilege. While that can be helpful when done correctly (though the protection is far from absolute), it is greatly underselling the real value that experienced legal counsel can add. When it comes to managing cyber risk, there is no substitute for experienced legal counsel leading the process.

Reasonable cybersecurity is a process, not a definition

Texas Attorney General Ken Paxton, explaining his office's role in the recently settled litigation against Neiman Marcus for its 2013 data breach, emphasized why Texas law requires businesses to have a cyber risk management program: "A business shall implement and maintain reasonable safeguards against cyberattacks to protect consumers' personal information from unlawful use or disclosure . . . . I urge companies to evaluate whether they have in place a thorough and ongoing written information security program that serves to safeguard their customers' information."[1] The law Attorney General Paxton is referring to is the Texas Identity Theft Enforcement and Protection Act, which specifically states "[a] business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information

[1] AG Paxton Announces $1.5 Million Settlement with Neiman Marcus over Data Breach, Jan. 8, 2019, (Press Release announcing settlement of State of Texas v. Neiman Marcus Group, LLC, Cause No. D-1-GN-19-000122, 98th Judicial District Court, Travis County, Texas. (Link to Settlement Agreement).

collected or maintained by the business in the regular course of business."[2] Even though the Attorney General's statement and the statutory language are short, determining what are "reasonable" safeguards and procedures is what most security managers and in-house counsel find challenging. They frequently ask, "but, what does reasonable mean?" They are looking for a definition or a simple checklist to say "this is reasonable." There is none. Determining what is reasonable is not a simple task and it must be made on a case-by-case by each business. There is no definition for reasonableness. "Reasonable" cybersecurity is a process, not a definition. That process is found in the cyber risk management program.

Real world experience for assessing and managing risk

To effectively manage cyber risk, companies must understand what their real cyber risk is because they cannot manage what they do not know or understand. Assessing a company's overall cyber risk is one of the most crucial steps in the risk management process. It is the foundation.

Attorneys who have substantial experience in dealing with cyber risk are able to better understand how to manage cyber risk, including legal and regulatory liability that leads to significant risk in this environment. Think about this: how many cyber incidents or data breaches has your company's information technology, security, and management teams been through or even observed first hand?

Counsel with many years of experience serving as a "breach guide" or "breach quarterback," leading companies through the cyber incident and data breach response process, will have been involved in hundreds or thousands of cyber incidents and data breaches. This real-world experience is invaluable for helping companies understand the real-world risks they are now facing. Without such practical experience, companies are more likely to spend their resources chasing some of the hyped-up threats that make the best sales pitches, conference talks and news headlines. But, it is not always the most exotic and sophisticated attacks that cause the most problems.

Diving deeper, such counsel will have a unique perspective on the most common attack tactics that have been used in the past and that are currently being used against certain types and sizes of companies, in certain industries, with certain types of data and business models, and in certain markets. They will also understand the types of attacks that are most likely to lead to reportable data breaches. They will have a better understanding of the laws and regulations

---

[2] Tex. Bus. Comm. Code § 521.052(a).

applicable to the jurisdictions in which the companies operate and what they require in terms of securing information, disclosing breaches of such information and the all-important question of distinguishing between a non-reportable incident and a reportable data breach, a subtle yet potentially bet-the-company distinction.

Deeper still, by calling on their history of cases, experienced counsel will have a unique understanding of those things that companies did right and those things that were ineffective or led to problems. Because no two companies are alike, this insight provides a deeper understanding of what caused many cyber incidents, how they happened and what could have prevented them. Once an incident has occurred, the focus shifts to an understanding of what companies did right or wrong, or could have done but did not do, that may have improved the response and better mitigated the situation. Finally, it enables them to uniquely understand the true harm to companies that such cyber incidents may cause, from the initial panic, administrative burden and confusion and disruption of operations, to the loss of business opportunities due to the companies being focused on the incident, to the better-known harms, such as the costs of remediation and incident response, negative publicity and the decrease in business value and stock prices.

Real world experience for developing strategy and prioritizing steps

When working with companies on their cyber risk management programs, one of the most frequently asked questions is, "how do you prioritize the steps in your strategic action plan?" Because companies cannot "boil the ocean" (*i.e.,* fix every problem) and do not have unlimited resources to throw at this problem, they must be able to evaluate the risks and develop a strategic action plan that prioritizes those things that should be done first. There is a lot more to consider than the traditional risk formula of "risk = probability x loss" because there are important business factors that must be considered. When evaluating how to prioritize the actions to take, the risk formula analysis should also take into account factors such as time and cost to implement, impact on the business and resources, and the benefits and hindrances of the proposed actions. To work through such an analysis requires not only drawing on real-world experience to understand the most likely risks companies face, but also an understanding of the overall business, its operational needs, the practicalities of the business environment and the many competing interests that must be considered. The analysis of such complexities is an essential skill for legal counsel.

With cyber risk, even the most extensive and effective risk management programs cannot come with guarantees. The problem is not a static problem that can be solved once and for all,

rather, it involves an active adversary that is continuously evolving its strategy and tactics to find more effective ways of attacking and exploiting its intended victims. And, as with security in general, the company must get it right 100% of the time and the attacker needs only one lucky shot. Because of the nature of the beast, when it comes to legal and regulatory liability, the question is usually not as simple as "did the company have a data breach?" but is more like "before the company had the data breach, was it taking reasonable measures to protect its network and data to keep from having a data breach?" Well-documented evidence of its diligence can go a long way in answering this critical question for regulators.

Privilege is valuable, but it must be done right

Not to be ignored, the attorney-client privilege can play an important role in many jurisdictions, such as the United States. However, because the privilege applies to communications and does not shield facts, it is not as effective or impenetrable as many think for either pre-incident risk management or post-incident response.

The best way to help ensure the privilege applies is to have the activities integrally intertwined with the rendering of legal advice by ensuring the attorney is retained first, then the attorney retains and directs the work of consultants and that counsel's role is prominent by truly leading the process so that the consultants are reporting to the attorney who is then using their work to render legal advice. Even then, however, there are no guarantees with privilege. The best course of action is to prepare by doing everything possible to have the privilege but carry out the work as though there will be no privilege because there might be none.

There is no substitute for experienced legal counsel in managing cyber risk. In today's business environment, cyber is unquestionably a technical issue as well as a legal issue, which requires experienced legal counsels to be integrally involved in helping companies manage their cyber risk.

About the Author

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

Cell Phone Tracking in Texas

By Pierre Grosdidier

In *Sims v. State*, the Texas Court of Criminal Appeals ("TCCA") unanimously held that authorities did not violate a suspect's Fourth Amendment privacy rights when they "pinged" his cell phone less than five times over less than three hours without a warrant to locate and arrest him on suspicion of murder.[1] The decision is consistent with *Carpenter v. United States*, where the U.S. Supreme Court recently held that a warrant was required to access seven days of cell-site location information (CSLI).[2] *Carpenter* was a narrow decision that left room for warrantless requests for CSLI under exigent circumstances, such as when authorities "need to pursue a fleeing suspect, [or] protect individuals who are threatened with imminent harm."[3]

Sims' grandmother was found dead from gunshot at her home. Her car, purse, and two handguns were missing. Relatives immediately suspected her absent live-in grandson of the crime.[4] Believing Sims to be armed and dangerous and acting without a warrant or even a court order, the police had the service provider proactively ping his cell phone to pin its location in "real-time."[5] The pings helped locate Sims, whom police arrested in possession of one of the guns, six knives, ammunition for a siege, and a blood-stained towel. At his trial for murder, Sims moved to suppress the real-time CSLI.[6] He eventually pleaded guilty and received a 35-year sentence, reserving the right to appeal the trial court's denial of his motion. The Texarkana Court of Appeals affirmed, and Sims petitioned the TCCA.

The TCCA followed *Carpenter*'s reasoning. In that case, the U.S. Supreme Court had "recognize[d] that CSLI is an entirely different species of business record," and it declined to extend the two lines of cases that have guided its Fourth Amendment data privacy analysis.[7]

---

[1] No. PD-0941-17, --- S.W.3d ---, 2019 WL 208631, at *8 (Tex. Crim. App. Jan. 16, 2019) (not released for publication).

[2] 138 S. Ct. 2206, 2217 n.3 (2018).

[3] *Id*. at 2220, 22-23 ("Our decision today is a narrow one.").

[4] *Sims v. State*, 526 S.W.3d 638, 640 (Tex. App.—Texarkana 2017) (*affirmed*).

[5] *Sims*, 2019 WL 208631, at **1-2 and n.1.

[6] Neither the appellate nor the TCCA opinions dwell on this point, but we can surmise that by suppressing the CSLI, Sims tried to suppress the evidence collected at the time of his arrest.

[7] *Carpenter*, 138 S. Ct. 2222.

The linchpin of this analysis is that the Fourth Amendment protects a person's subjective expectation of privacy "that society recognizes, or is prepared to recognize, as reasonable."[8]

The first line of U.S. Supreme Court cases analyzed the legality of physical tracking devices. Under the public-thoroughfare rule, a "beeper" placed in a jug of chloroform that, along with visual surveillance of its ferrying vehicle, led authorities to a methamphetamine lab was held not to violate the Fourth Amendment. The court reasoned that the car's peregrinations on public roads was for all to see and the beeper conveyed only a limited amount of information.[9] But, a GPS tracking device attached to a car for 28 days constituted a Fourth Amendment search, even if some of the travels occurred in public view.[10] The second line of cases, which grew into the third-party doctrine, established that individuals have a reduced expectation of privacy in information that they knowingly share with others, such as bank records or phone numbers dialed from a home land line.[11] The Court held that the doctrine did not apply to CSLI because these records were not voluntarily surrendered to a service provider as were bank records or dialed numbers.[12]

Applying *Carpenter*, the TCCA held that whether a CSLI grab constituted a Fourth Amendment search turned on the amount of data seized. "There is no bright-line rule" and every situation "must be decided on a case-by-case basis."[13] But, in this case, fewer than five real-time pings in under three hours were insufficient to breach a person's reasonable expectation of privacy.[14]

Importantly, the Court declined to find a difference between historical CSLI records, as in *Carpenter*, and Sims' real-time records, obtained by pinging his phone. A person's expectation of privacy turned on the measure of the invasion, which in this case corresponded to the amount of data seized.[15] Sims was nabbed with a few pings in barely three hours, but the police might want to track a suspect in real-time "for days or even weeks." Impliedly, a warrant would then be required, as with the GPS tracker in *Jones*. The reverse logic raises the important question of how much historical CSLI triggers the need for a warrant. It might only take a few

---

[8] *Sims*, 2019 WL 208631 at *6 (citing *Katz v. United States*, 389 U.S. 347 (1967).

[9] *Id*. (citing *United States v. Knotts*, 460 U.S. 276 (1983).

[10] *Id*. at *7 (citing *United States v. Jones*, 565 U.S. 400 (2012).

[11] *Id*. (citing *United States v. Miller*, 425 U.S. 435 (2012) (bank records); *Smith v. Maryland*, 442 U.S. 735 (1979) (phone numbers)).

[12] *Id*.

[13] *Id*.

[14] *Id*. at *8.

[15] *Id*. at *7 n.15.

minutes of well-timed historical CSLI from a small cell to confirm a person's presence in a locale to destroy an alibi or substantiate a suspicion. Will such a circumscribed inquiry require a warrant?

About the Author

Pierre Grosdidier is Counsel in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. Pierre divides his practice between construction litigation and construction contract drafting. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, a registered P.E. in Texas (inactive), and the State Bar of Texas Computer & Technology Section Webmaster and Circuits eJournal Co-Editor for 2018-19.

Mining for Virtual Gold: Understanding the Threat of Cryptojacking[1]

By Stephen Viña

Instead of stealing company data or holding it ransom, cyber criminals have mastered a new way to attack businesses. Through cryptojacking, criminals can siphon an organization's computing power to mine cryptocurrency, opening the door to new sources of illicit revenue at the company's expense. And, your organization may already be a victim and not even know it.

What is Cryptojacking?

Thousands of cryptocurrencies or "coins" exist today, all with varying purposes. Some, such as Bitcoin and Monero, serve as a digital currency and can retain considerable monetary value. The all-time high for a single Bitcoin, for example, peaked around $20,000 in December 2017 and then proceeded to lose much of its value over the course of 2018. Creating Bitcoin and Monero, and other cryptocurrencies, requires the completion of a complex cryptographic puzzle that is recorded on a blockchain, a process known as cryptomining. Performing these calculations can be expensive, requiring considerable processing and electrical power and, in some cases, special equipment. For their efforts, miners are rewarded with newly created units of the mined cryptocurrency, providing a potentially lucrative pay day depending on the value and quantity of the coin.

---

[1] *Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman. This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.*

As the value of cryptocurrencies soared in 2017, organizations turned to coin mining as a new source of revenue. For example, some companies, asked online users whether they would allow their computers to be used to mine cryptocurrency in exchange for eliminating advertisements. Others, however, simply decided to steal or "hijack" the necessary computing power from unsuspecting consumers and businesses. What was once a complicated process has become relatively easy with the advent of in-browser mining scripts that allow scammers to use the computing power of anyone who visits an infected website. Cryptomining malware can also be spread through malicious links, advertisements, email attachments, public Wi-Fi, fake apps, and system backdoors.

Infections were rampant last year. For example, in February 2018, hackers compromised a screen-reading web plugin for the blind, affecting over 4,000 websites worldwide, including the UK's National Health Service.

Some companies represent particularly strong targets for cryptojacking. These include:

- Critical infrastructure companies, which consume significant amounts of power and often have vulnerable industrial control systems.
- Companies that rely heavily on cloud services, which present the opportunity for "high-powered mining."

Cryptojacking is also frequently tied to Internet of Things (IoT) devices such as mobile phones, which can allow miners to quickly amass armies of hijacked devices to mine cryptocurrency at scale.

How Cryptojacking Can Affect Businesses

The theft of company computing power through cryptojacking can have real financial consequences over time. Accurately capturing the direct costs of cryptojacking; however, may prove difficult, since victims may not notice an infection or recognize the culprit.

But, the threat is real. An infected computer system could become sluggish due to the complex and continuous number-crunching operations required to resolve mining calculations. Overworking computers could cause necessary functions to crash and, in some cases, lead to overheating and the ultimate failure of central processing units (CPUs). This problem may seem like a temporary or isolated nuisance, but spread across a corporate enterprise, it could have disruptive and costly implications for companies. Indeed, insurers are already seeing cryptojacking claims related to unusually high CPU usage and other IT complications, such as email system compromise.

In addition to the potential degradation in service and resulting lost productivity and income, businesses may incur costs for higher energy consumption or cloud usage. An organization could also incur extra expenses for replacing hardware sooner or more frequently than planned, and needing more extensive IT support to address slow performance or remediate systems. Cryptojacking malware may also impact company defenses, making the organization more susceptible to other malware.

Companies that transfer cryptomining software to unsuspecting third parties have also become the subject of litigation and regulatory scrutiny. In 2018, the Federal Trade Commission (FTC), for example, launched a system for consumers to file complaints if they become victims of cryptojacking. The FTC has also brought enforcement actions against companies that have hijacked consumers' mobile devices with malware to mine virtual currency.

Can Cyber Insurance Help?

Cyber insurance policies are designed to cover both direct loss and liability caused by a cyber event. Cyber policies can cover expenses incurred directly by policyholders for IT forensics, recreation or restoration of data assets, data breach response, and loss of business income. Coverage also extends to third-party liability claims for privacy breaches and security failures, such as the transfer of malware to a third party or the unauthorized disclosure of sensitive customer data.

A cryptojacking incident may result in several types of losses that could be covered under cyber insurance policies. For example, a cryptojacking event could disrupt important control systems or a company network, triggering business interruption coverage. Cyber insurance may also help cover costs for investigations to determine the cause, source, and scope of a cryptojacking incident. Companies that unwittingly pass cryptojacking malware to third parties may also look to a cyber insurance policy for relief from any related claims for damages.

Whether cyber insurance responds will depend upon the specific terms and conditions of a given policy, as well as the actual claims application. Businesses should consider carefully reviewing specific coverage provisions to determine whether and how their policies will react to cryptojacking losses. Businesses should also work with their risk advisors and legal counsel to ensure that their cyber policies include specific claim triggers and broad definitions of loss in order to capture all possible scenarios for which an insured would expect to recover loss.

As long as there is big money to be made, cyber actors will likely continue to hijack computer systems to mine cryptocurrency, evolving their methods along the way. Like other

cyberattacks, businesses should look to detect and prevent this growing and evolving threat and assess insurance policies for potential recovery.

About the Author

Stephen Viña is a Senior Vice President and Advisory Specialist in the Cyber Center of Excellence at Marsh, a global insurance brokering and risk management firm. He can be reached at Stephen.Vina@marsh.com.

Genetic Data Privacy: Notable Practical and Legal Developments in 2018

By William D. Smith

2018 saw an increase in public awareness of genetic data due to several high-profile news stories where consumer genetic test databases helped solve decades old crimes, most notably the Golden State Killer case.[1] The popularity of such consumer genetic tests has also grown rapidly, with the number of individuals using them expected to exceed 20 million this year.[2] This article first outlines some of the practical and commercial changes in how genetic information is collected and used. It then examines a selection of U.S. and international legal developments in 2018 relating to genetic data. There are many different laws, regulations and industry standards governing the collection and use of genetic data. However, the importance of de-identification or anonymization is a common feature that is frequently key to using this data in a compliant fashion. Courts and practitioners will increasingly be asked to define and advise on how to handle de-identification, as use of genetic data becomes more prevalent in business, medicine, law, and individuals' personal lives. Since caselaw on de-identification and genetic data remains sparse, this article also reviews a recent case dealing with de-identification outside the genetic context that examines principles that might also be applied to the de-identification of genetic data.

Genetic Data is Unique

Genetic information is distinct from other categories of personal data in three ways. First, genetic data is fixed for a person's entire lifetime. Second, the information provided by genetic data (particularly full genome sequencing) may continue to grow significantly after it is collected, as technology expands our understanding of different genes and gene combinations. These characteristics create challenges in applying notions of notice, informed consent, and other legal and ethical concepts, because the full significance of the provided or gathered data cannot be known at the time of collection. Third, genetic data is unique from a privacy law and individual rights perspective, as it contains information about the subject's blood relatives, including kinship and heritable traits. Genetic data is, therefore, potentially far more broadly incriminating than fingerprints.

---

[1] Natalie Ram *et al.*, *Genealogy databases and the future of criminal investigation*, Science June 8, 2018, at 1078.

[2] MIT Technology Review https://www.technologyreview.com/s/612281/look-how-far-precision-medicine-has-come/, October 23, 2018.

A common way to deal with these challenges is to try to anonymize the genetic data so that individuals whose data is stored cannot be identified. However, among sources and users of genetic data there is often a lack of appreciation for what can be inferred from these data sets, and what potentially corroborating data are available.[3] As far back as 2007, the National Institutes of Health warned that technology made the identification of specific individuals from raw genetic data increasingly feasible.[4]

The Law is Evolving, but Not as Quickly as the Industry

Genomic data analysis was initially the purview of governments and large institutions because of its cost and complexity. Governments established DNA "fingerprinting" databases, which have been used to match biological evidence to a sample from a particular suspect, and the regulations for using these databases. Many jurisdictions also adopted laws designed to prevent discrimination based on genetic information by employers or insurers, such as the U.S. Genetic Information Nondiscrimination Act of 2008 (GINA).[5] Today, collection and use of genetic data in consumer genetic testing, law enforcement, and medical research goes beyond what was contemplated when existing statutory/regulatory frameworks were first created. Lawmakers will eventually catch up. In the meantime, self-regulatory frameworks are being released, discussed below, that may establish the foundation for governmental standards when they do come.

Consumer Genetic Testing

Most readers are aware of the relatively inexpensive genetic tests available from private-sector providers such as 23andMe and Ancestry. These tests allow individuals to submit a DNA sample and have it analyzed to gain insights about their health, their family tree, and other personal characteristics. The market for these services is projected to triple in size from 2017

---

[3] Kuchinke, Wolfgang *et al.*, "Development Towards a Learning Health System Experiences with the Privacy Protection Model of the TRANSFoRm Project", in Serge Gutwirth *et al.*, Eds. *Data Protection on the Move*, Springer 2016, p.121.

[4] National Institutes of Health, Policy for Sharing of Data Obtained in NIH Supported or Conducted Genome-Wide Association Studies (GWAS) (Aug. 28, 2007), https://grants.nih.gov/grants/guide/notice-files/not-od-07-088.html.

[5] Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. § 2000ff *et seq.*; *see also* Survey of European laws against genetic discrimination in Van Hoyweghen, "National legal and policy responses to genetic discrimination in Europe", Gerard Quinn *et al* eds., *Genetic Discrimination: Transatlantic perspectives on the case for a European-level legal response,* Routledge 2015 p.199.

to 2022.[6] The traditional research/medical principle of informed consent is difficult to apply in this context, because individuals who submit their genetic data may be provided with information they and those processing their data did not expect nor can they predict. A user may submit a sample out of curiosity about family history, a desire for predictions about health outcomes, mere entertainment, or all of the above. In some cases, the outcome of the test may not be intended at all. For example, in 2017 a man accidentally discovered that he had a half-brother after submitting a genetic sample for testing. This revelation ultimately led to his parents' divorce.[7]

New Uses of DNA by Law Enforcement

Law enforcement organizations around the world have been quick to recognize the utility of these new sources of genetic data. Even though the arrest of the suspected Golden State Killer in the spring of 2018 was not the first time authorities used a consumer genetic database to apprehend a suspect, the incident significantly raised public awareness of this technique. Investigators in that case matched DNA recovered from crime scenes with DNA information uploaded by a relative of the suspect to a free online genetic database called GEDmatch.[8] A number of states require certain criteria to be met to permit a familial search of their government-maintained DNA databases. For example, in Texas, the DPS policy indicates that the investigation must be of a serious crime and that other avenues must have been exhausted.[9] These requirements do not apply to the use of publicly available databases such as GEDmatch. But, the implicit rationale, that the data subject voluntarily publicized this information, does not apply if the actual data subject of interest is a family member of the DNA sample source, as was the case in the Golden State Killer case.[10] Interestingly, in 2012, a group advising EU Member States called PHGEN II considered this question in the healthcare context—should close blood relatives be considered data subjects along with the actual person providing the DNA sample—and concluded that due to the complexity granting such rights

---

[6] Fasken Martineau DuMoulin LLP, https://www.fasken.com/en/knowledgehub/2018/09/privacy-cybersecurity-bulletin-genetic-testing-and-privacy, September 13, 2018.

[7] Tonic https://tonic.vice.com/en_us/article/gve83w/when-an-ancestry-test-tells-you-your-dad-isnt-your-dad April 7, 2017.

[8] Natalie Ram *et al.*, supra, p. 1078.

[9] Texas DPS: Combined DNA Index System Local Laboratory Familial Search Request Checklist https://www.dps.texas.gov/CrimeLaboratory/Pubs.htm.

[10] Natalie Ram *et al.*, supra, p. 1078.

would create, relatives should not be considered data subjects in that context.[11] As public awareness of these techniques increases, there may be calls for more controls. In the meantime, the public scrutiny of the Golden State Killer case led the genetic testing industry to issue voluntary Best Practices, discussed below.

Governments have maintained DNA databases for investigation purposes for many years—for example the U.S. National DNA Index System (NDIS) currently contains more than 12 million DNA profiles.[12] However, the use of DNA phenotyping and the storage of DNA records of individuals not convicted of a crime raise new legal questions.

Historically, DNA evidence was used for "DNA fingerprinting," which is the comparison of DNA evidence from a crime with the DNA profile of a suspect to confirm or eliminate them. Today, investigators are beginning to use DNA evidence for "DNA phenotyping." The term refers to the use of genetic information to attempt to predict the likely ancestry, physical features, or other identifiable characteristics of the unknown source of the genetic information. Last summer, the German state of Bavaria adopted a measure to approve use of DNA phenotyping in cases where there is an imminent danger of a crime being committed in the future.[13] Many of the techniques contemplated in this new law were developed by a research team at Erasmus University in the Netherlands working with universities in the United States. For example, Purdue University in Indiana released a tool called HIrisPlex-S that can return probabilities for three eye colors, four hair colors, and five skin shades based on a DNA sample. The goal is to enable investigators to narrow the range of potential suspects using these projected characteristics based on crime scene DNA evidence.

U.S. law enforcement authorities are also using DNA phenotyping techniques on an *ad hoc* basis, in the absence of permissive or restrictive regulation on the subject. Service providers such as Parabon Nano-Labs even offer solutions that purport to generate a facial sketch based on DNA samples.[14] The lead researcher of the Erasmus University team rejects the scientific validity of that approach, which he said exceeds the current state of the science.[15] However,

---

[11] Future of Privacy Forum: Best Practices for Consumer Genetic Testing Services p. 17.https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf July 31, 2018.

[12] Natalie Ram *et al.*, supra, p. 1078.

[13] Gretchen Vogel, *German law allows use of DNA to predict suspects' looks*, Science, May 25, 2018, at 841.

[14] Parabon Nano-Labs https://snapshot.parabon-nanolabs.com/.

[15] Gretchen Vogel, *supra*, at 841.

according to testimonials on Parabon Nano-labs' website, this service has been used by more than 25 local and state law enforcement organizations in the U.S., including Texas police and sheriff's departments in Arlington, Brown County, Fort Worth, Galveston and League City.[16]

As the collection and use of DNA by law enforcement agencies has become more widespread, courts and lawmakers have wrestled with the question of how to deal with DNA samples obtained from individuals other than those convicted of serious crimes. In 2013, the Supreme Court confirmed that law enforcement collection of DNA samples from individuals not yet charged with a crime was lawful.[17]

That case, *Maryland v. King*, concerned Alonzo King, who was arrested in 2009 for assault. During his booking, police took a cheek swab and King's DNA record was uploaded to the Maryland DNA database.[18] The database matched King to a DNA sample from an unsolved 2003 rape. After he was charged for the rape, King sought to suppress the DNA evidence based on Fourth Amendment grounds. King's Fourth Amendment argument was rejected by the trial court and he was convicted, but the Maryland Court of Appeals agreed and invalidated the part of the Maryland DNA collection law that permitted collection of samples from arrestees as unconstitutional.[19] In a 5-4 decision the Supreme Court reversed the Maryland court's judgment.[20] The Court stressed that reasonableness rather than specific individual suspicion is the key Fourth Amendment requirement.[21] It concluded that in the context of an otherwise valid arrest, a cheek swab represents only a "minor intrusion" on the suspect's expectations of privacy, while the state has significant interests in identifying the suspect.[22] Because state interests prevailed, the majority held, taking a DNA sample, "like fingerprinting and photographing" is "a legitimate police booking procedure that is reasonable under the Fourth Amendment."[23]

The retention of DNA profiles after an arrestee is cleared, or where the status of a conviction has changed retroactively, raises other questions, however. In a recent case discussed below, the Supreme Court of California addressed the intersection of DNA database expungement

---

[16] Parabon Nano-Labs https://snapshot.parabon-nanolabs.com/testimonials.
[17] *Maryland v. King*, 569 U.S. 435, 465 (2013).
[18] *Id*. at 441.
[19] *Id*. at 442.
[20] *Id*. at 466.
[21] *Id*. at 448.
[22] *Id*. at 465.
[23] *Id*. at 466.

rights and the retroactive re-classification of offenses. Given that both collection of DNA by law enforcement and re-categorization of offenses like marijuana possession are ongoing trends, this question is likely to arise elsewhere.

In re C.B. (Cal. 2018)

On August 30, 2018, the Supreme Court of California issued an opinion in a consolidated case dealing with two defendants, C.B. and C.H., who sought to have their DNA samples removed from the California Department of Justice's DNA databank.[24] C.B. and C.H. had been convicted of various theft, burglary, and assault offenses, and ordered to submit DNA samples. Collection of the DNA samples was required pursuant to the California DNA and Forensic Identification Data Base and Data Bank Act of 1998, as amended by Proposition 69 in 2004, because the defendants' offenses were felonies. Subsequently, in 2014, California voters passed Proposition 47, which reclassified various drug and property offenses from felonies to misdemeanors.

After this reclassification, C.B. and C.H. "petitioned to have their felony violations re-designated as misdemeanors, their fines reduced, and their DNA samples and profiles expunged from the state databank." The trial courts granted the requests for re-designation and fine reductions, but denied the motions for expungement. Different panels of the Court of Appeal affirmed.

C.B. and C.H. argued that since Proposition 47 provides that "a felony conviction that is […] designated as a misdemeanor under subdivision (g) shall be considered a misdemeanor for all purposes," their offenses no longer obligated them to submit DNA samples and the samples they submitted in the past should therefore be expunged. After a textual analysis of California Penal Code Section 299, which governs retention and expungement of DNA samples/profiles, and comparing it to Section 296, which governs the requirement to submit DNA samples, the Supreme Court of California concluded that the defendants did not meet all of the criteria for expungement. Under Section 299, expungement is only permitted if "(1) charges were either not filed or were dismissed, (2) charges resulted in an acquittal, (3) any conviction was reversed and the case dismissed, or (4) the petitioner was found factually innocent."[25] The court found that the reclassification of the offense did not satisfy any of these criteria, and

---

[24] *People v. C.B. (In re C.B.)*, 425 P.3d 40 (Cal. 2018) https://www.courts.ca.gov/opinions/archive/S237801.PDF.

[25] *Id.* at 46.

accordingly expungement was not authorized, leading the court to affirm the judgment below.[26]

The court also rejected a series of statutory purpose arguments made by the defendants about the history of Proposition 47, and federal and California equal protection clause arguments. Even though these arguments were not essential to the holding, it is interesting to note that, in rejecting the statutory purpose argument, the court endorsed prior California cases finding that "requiring the submission of a sample is not punishment." It seems possible that, as the significance of genetic data is better understood, the notion that there is nothing punitive about compelling its submission will be revisited. Finally, in a concurring opinion, Justice Liu noted that neither defendant "pressed any claim that the state's retention of his DNA samples implicates a constitutionally protected privacy interest" and held open the door for a different result in a future case along those lines.[27]

Genetic Data and Medical Research

Medical scientists and biopharmaceutical companies are investing significantly in "precision" or "personalized" medicine. Personalized medicine seeks to match treatments to the genetic profile of a specific patient, to improve effectiveness and reduce side effects. Personalized medicine has been in development since the Human Genome Project in the 1990s, but the reduction in cost to sequence a human genome—from over $95 million in 2001 to under $1,200 in 2017—means that this research is much more common today.[28] Developing personalized medicine requires large-scale analysis of genetic and health data to match disease characteristics, treatment response, and incidence of side effects to particular genetic markers. As a result, companies and other researchers are processing massive amounts of genetic data and associated individual health information.

The handling of this data processing in compliance with ethical and legal requirements hinges on de-identification. This de-identification process is usually completed by the clinical trial recruiter or other collectors of the genetic information before it is handed over to the research group.[29] Traditionally, those sources are places like university-run research hospitals with a well-established culture of medical/research ethics. Oversight of privacy law compliance often

---

[26] *Id.* at 51.

[27] *Id.*

[28] MIT Technology Review https://www.technologyreview.com/s/612281/look-how-far-precision-medicine-has-come/ October 23, 2018.

[29] Author's interview with anonymous postdoctoral genetics researcher in industry, October 24, 2018 (Interview October 24, 2018).

sits with the group responsible for medical ethics and collaboration review.[30] However, the imperatives of medical ethics (which emphasize consent to treatment interventions and prioritize health outcomes) and personal data protection (which emphasize an individual's property rights in his or her data) are not always the same. As privacy law becomes more fleshed out in many jurisdictions the tension may increase.

Research companies and institutions are also broadening the range of sources from which they acquire genetic data, including most notably consumer genetic testing companies. This summer GlaxoSmithKline announced an investment in 23andMe and a partnership that gives the drug company research access to the genetic data of 23andMe customers.[31] 23andMe acquires consent for research use from customers submitting DNA samples, and customers can revoke that consent. However, privacy activists such as Dr. Arthur Caplan raised questions about how informed it is and if consumers fully understand what they are agreeing to.[32] Also, the shared assumptions and culture that underpin the exchange of medical data between research scientists and traditional sources like research hospitals may not exist when the source is a consumer technology company informed by the world of startups and software.

In this environment, where scientific technology and commercial practice have moved more quickly than legislation, the vacuum is being filled by self-regulatory frameworks. Two notable examples have been established in the second half of 2018.

Future of Privacy Forum: Privacy Best Practices for Consumer Genetic Testing Services

On July 31, 2018, the Future of Privacy Forum (FPF), an industry group and think tank, promulgated a set of Best Practices to govern how genetic testing companies should handle the privacy of their customers and genetic data.[33] The Best Practices were clearly influenced by the approach utilized in the European Union General Data Protection Regulation (GDPR), and are oriented around the principles of: (1) Transparency, (2) Consent, (3) Use and Onward Transfer, (4) Access, Integrity, Retention and Deletion, (5) Accountability, (6) Security, (7) Privacy by Design, and (8) Consumer Education. The specific requirements in each of these categories will be familiar to those who have reviewed the GDPR or the California Consumer Privacy Act, such as the need to give users clear notice of how their data will be used, to acquire consent for

---

[30] *Id.*

[31] Time Magazine http://time.com/5349896/23andme-glaxo-smith-kline/ July 26, 2018.

[32] *Id.*

[33] https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf.

each specific new use, to allow data subjects to exercise rights to access and delete their data, and so forth.

Notable are the exceptions from the default rules. De-identified information is not subject to the restrictions in the Best Practices "provided that the deidentification measures taken establish strong assurance that the data is not identifiable".[34] This section notes that, even if de-identified, genetic data held at the individual level "cannot be represented as strongly protecting individuals from re-identification." "New product development" is also an important exception in the Best Practices. New product development is considered an "inherent contextual use" of the collected data. So while initial express consent is required for it at the time of signup, informed consent for research is not required when the purpose of the research is new product development by the testing company.

Major players in the industry such as Ancestry and 23andMe have committed to following these policies.[35] Given that FPF has taken the "first mover" advantage by producing these Best Practices in advance of any statute or regulation dealing with consumer genetic testing in detail, it seems likely that at least portions of this framework will become the basis for more binding rules in the future. The Best Practices document also contains two useful appendices with a summary of what FPF sees as the key legal and regulatory guidance impacting genetic testing (Annex B), and a list of genetic data sharing policies promulgated by NGOs and similar groups (Annex C). Annex C is interesting because it lists guidelines that are not laws or regulations and may fall under the radar of legal practitioners. However, they inform day to day decision-making by doctors and researchers working in the industry.

UK Code on Genetic Testing and Insurance

In a more formalized example of self-regulation of genetic data use, since 1997 the UK insurance industry has been subject to a binding but voluntary series of instruments restricting the use of genetic data and testing in the insurance context. That arrangement was renewed in October in the form of a Code on Genetic Testing and Insurance.[36] The Code prohibits insurers from requiring a genetic test as a precondition to obtain insurance, and requires that results of

---

[34] Future of Privacy Forum: Best Practices for Consumer Genetic Testing Services.

[35] Washington Post https://www.washingtonpost.com/technology/2018/07/31/ancestry-andme-others-say-they-will-follow-these-rules-when-giving-dna-data-businesses-or-police/?utm_term=.72bf44bd7714, July 31, 2018.

[36] HM Government, Code on Genetic Testing and Insurance. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/751230/code-on-genetic-testing-and-insurance.pdf.

a predictive genetic test may only be considered in specified circumstances and for policies above a certain monetary size. At the moment, the only approved instance is a predictive genetic test for Huntington's disease, which can be considered in applications for life insurance cover of £500,000 or more. This list could be expanded by the Association of British Insurers in the future. Interestingly, it also requires all insurers offering covered lines of business to nominate "at least one appropriately trained genetics underwriter."

The Code employs a firm distinction between diagnostic genetic tests, which "confirm or rule out a diagnosis based on existing symptoms," and predictive genetic tests, which "predict a future risk of disease in individuals without symptoms of a genetic disorder." However, as the technology becomes more sophisticated and the range of products offered by genetic testing companies grows, this distinction may become blurred.

Regulatory Frameworks Hinge on De-identification

Many statutes, regulations, and policies governing data privacy generally do not specifically define standards for de-identification. (Emphasis added in each of the following quotations). The GDPR provides that it should not apply to data that is not identifiable to an individual natural person.[37] To determine if data that has undergone pseudonymization is identifiable "account should be taken of all the means reasonably likely to be used." California's new Consumer Privacy Act defines "de-identified" information as that that "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer," subject to additional organizational controls by the business.[38] Under the HIPAA Privacy Rule, the standard for de-identification provides that de-identified information is not protected health information if "there is no reasonable basis to believe that the information can be used to identify an individual."[39] Even though the Privacy Rule offers one safe harbor method that delineates a specific set of de-identification steps, it alternatively permits the use of any other method if it meets that standard and is endorsed by an appropriate expert.

Practical frameworks that do not have the force of law but govern the day-to-day sharing of genetic data in healthcare and industry often do not specify methods for de-identification. The European TRANSFORM project seeks to enable scientific researchers to use data from primary

---

[37] Recital 26 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.

[38] Cal. Civ. Code § 1798.140(h).

[39] 45 CFR 164.514; see also https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

care physician visits. Even though its operating model includes a detailed concept of "privacy zones" and other mechanisms to protect patient data, and requires de-identification at various points of data exchange, it does not specify particular means for de-identification.[40] FPF's Privacy Best Practices (see above) define de-identified information as information that "cannot reasonably be associated with an individual."[41]

Sander v. State Bar of California (2018)

Data collection/processing technology and statistical analysis techniques are rapidly evolving, so it is not surprising that lawmakers and regulators have leaned on a reasonableness standard in this area. However, that approach will likely lead to courts and other fact finders being asked to evaluate the quality and appropriateness of de-identification methods when data breach litigation or other disputes arise. The following case decided by the California First Appellate District in August 2018 is not about genetic data, but the opinion does contain a rare detailed inquiry into de-identification techniques. It is also particularly relevant to lawyers, as it concerns disclosure of records in the California bar admissions database.

Sander concerned a request by a public interest group for bar records from all applicants to the California Bar Examination from 1972 to 2008.[42] The petitioner sought this data to enable it to study a potential relationship between preferential university admissions programs and bar passage rates among racial and ethnic groups. After a complex procedural history and remand, the case went back before the California First Appellate Division. On remand, the trial court had sought to evaluate "(1) whether the requested information can be provided in a form that protects the privacy of applicants and (2) whether countervailing interests outweigh the public's interest in disclosure."[43] Ultimately, the court resolved the issue based on the fact that the California Public Record Act does not require a public agency to create *new* records in response to a public request.[44] Since each of the methods proposed by the petitioners for rendering de-identified data would require the creation of new records, the court denied the request.

However, *Sander* contains a detailed summary of trial expert testimony from Dr. Latanya Sweeney about the risk of re-identification for each of four alternate methods or "Protocols" of

---

[40] Kuchinke, *supra*, p.109.
[41] Future of Privacy Forum Best Practices.
[42] *Sander v. State Bar of Cal.,* 237 Cal. Rptr. 3d 276, 280 (Cal. App. 2018).
[43] *Id*. at 280.
[44] *Id*. at 288.

de-identification proposed by the petitioners to enable them to receive the Bar applicant records.[45] Protocol One would have the State Bar create a physical safe room where research could be conducted under the supervision of the Bar. Protocol Three employed a complex set of statistical transformations that changed the data so radically that the petitioners felt it would no longer be usable. The other two Protocols were based on the concept of "k-anonymity", developed by Dr. Sweeney, which measures the level of anonymity of a data set by counting the number of indistinguishable records within it.[46] In other words, in a data set with a k-anonymity of 20, any re-identification effort could not narrow down the set of possible "matches" to a known individual to less than 20. Protocols Two and Four were based on deleting portions of the database and grouping categories together (e.g., instead of a record showing graduation year 1974, it would show graduation band 1972-1975) until the k-value was 11. The expert concluded that each of these methods "presents cognizable risks that individuals may be specifically identified in the data."[47]

As noted above, the court did not reach the question of whether this risk of re-identification was acceptable under the balancing test. Instead, it resolved the case by affirming the trial court's first ground for denying the petition, that it would require the creation of new records, which is not authorized under the California Public Records Act. *Sanders* does not deal with genetic data. But, the analysis of de-identification techniques in the underlying litigation could provide a useful framework for practitioners seeking to attack or defend the "reasonableness" of de-identification methods applied to genetic data.

Conclusion

Consumer genetic testing grew in popularity in 2018. At the same time the use of genetic data by researchers and law enforcement expanded. Societies and governments will continue to wrestle with the questions of what restrictions and privacy protections are appropriate for this kind of information. Self-regulatory frameworks such as the FPF Best Practices, and the treatment of de-identification issues in other contexts, may provide clues as to the future development of law in this area. Current trends suggest that genetic science and consumer demand for genetic data processing will continue to advance regardless.

---

[45] *Id.* at 282.
[46] *Id.* at 283.
[47] *Id.* at 284.

About the Author

William Smith is Assistant General Counsel of Business Talent Group, LLC (BTG), the leading marketplace that connects independent management consultants, subject matter experts, and executives with top companies to solve their biggest business problems. He leads BTG's data privacy compliance, employment law, and commercial agreements activities. In addition, he closely supports BTG's General Counsel on fundraising transactions, governance and investor matters, and risk management. He is a member of the Council of the Computer and Technology Section of the State Bar of Texas.

Facing up to the FaceTime Bug

By John G. Browning

Touting its new wares on a giant Las Vegas billboard ahead of the massive annual Consumer Electronics Show (CES) in January, Apple proudly proclaimed "What happens on your iPhone, stays on your iPhone." Unfortunately, that privacy-centric marketing was soon undermined by revelations of a bug in Apple's iOS 12.1 iPhone software that lets outsiders eavesdrop on conversations being held during live video group chats using the company's popular FaceTime App. The "FaceTime bug," as it is now known, would occur when a user initiated a FaceTime Video call with an iPhone contact, and then while the call was dialing added his/her own number through the "Add Person" feature. This would allow the user to automatically begin hearing the other person's audio even before they accepted the call. The other person wouldn't be aware that the caller could hear them. In addition to such eavesdropping, the glitch also allowed video to be sent if the other user clicked either the "Power" button or one of the volume controls.

The privacy concerns and potential damage are obvious: one can listen in on soundbites of any iPhone user's ongoing conversation without their knowledge. But it would take a 14-year-old from Catalina, Arizona, Grant Thompson, to expose this security flaw. Apple disabled the group FaceTime feature while it investigated the bug and came up with a fix, but it took several emails and calls from Grant (who discovered the problem while using FaceTime to discuss Fortnite strategy with friends) and his mother to alert Apple to this vulnerability. Now, Apple reports that it has fixed the bug with a new software update and it has rewarded young Grant with an undisclosed sum of money, as well as an additional gift towards his college education.

However, it would not take long for the damages that such a security flaw could pose to attorneys' confidential and privileged communications to manifest themselves. On January 28, 2019, Houston criminal defense attorney Larry D. Williams, II filed a product liability and negligence lawsuit against Apple in Harris County state court. Williams alleges that he "was undergoing a private deposition with a client when the this [sic] defective product breach allowed for the recording of a private deposition." Williams' suit doesn't provide additional details about the case or client that was involved in the deposition, but does claim that as a result of Apple's flaw he's suffered "permanent and continuous injuries, pain and suffering and emotional trauma," as well as "lost ability to earn a living," "mental anguish, physical pain and

suffering, diminished capacity for the enjoyment of life, a diminished quality of life, and damages." The lawsuit asserts causes of action against Apple that include not just negligence and products liability for the alleged design defect and failure to warn consumers, but also breach of express and implied warranties, fraudulent concealment, fraudulent misrepresentation, negligent misrepresentation, unjust enrichment, and seeks compensatory and punitive damages. Williams' lawyer in this case is a Houston attorney, James C. Mattox, III, who clearly envisions bigger things, claiming that "An unknown number of undefined Plaintiffs have sustained similar privacy injuries as a result of the product."

Williams' lawsuit alleges that Apple had access to testing, research, and other data about the potential for such a flaw; and despite the fact that the tech giant knew or should have known about the dangers of such a bug, Apple failed to notify the public or take other appropriate steps. And while one can only speculate about the lawsuit's prospects for success, the timeline for the FaceTime bug raises questions about what Apple knew and when. Grant Thompson discovered the bug on January 19, and on January 20 his mother (a lawyer) sent a warning about it to Apple support. When she didn't hear back right away, she followed up with emails and faxes to Apple's security team and also posted on Facebook and Twitter. Yet it wasn't until January 25 that Apple's product security team instructed Thompson to create a developer request in order to submit a formal bug report.

The implications for lawyers of a privacy breach such as that described by attorney Williams in his lawsuit are clear. Texas Disciplinary Rule of Professional Conduct 1.05 discusses the importance of maintaining the confidentiality of attorney-client communications. And even if the "sworn deposition testimony" Williams was taking at the time might have become part of a public record at some point in the future, one cannot overlook the fact that eavesdropping by a third-party on FaceTime was invasive of Williams' work product on behalf of a client. Lawyers must be vigilant about both the risks and benefits of technology, just to be considered competent in their representation of clients. This not only means safeguarding one's confidential communications and work-product, but adopting cybersecurity measures in other aspects of an attorney's practice. Consider, for example the recent case of Panama City, Florida attorney Albert Sauline. Sauline contracts with an out-of-state company to do his social media marketing, including Facebook posts. Yet in late January 2019 Sauline was shocked to learn that his firm's Facebook page posted a photo of his business card with the message "Drunk in the middle of the night, all because the woman led you on all night for free drinks then wouldn't keep her promise after the club? Call Attorney Sauline "where we understand the tease." The post also tagged Sauline's personal Facebook page.

The post ignited a firestorm of critical comments, mostly from women. Sauline has deleted the "disgusting" post and maintains that after consulting with his marketing firm and changing the account's passwords, "It looked like someone was hacking our system." Yet such an episode underscores the importance for attorneys of keeping a close eye on their online presence and marketing efforts. Whether it's a security flaw like the FaceTime bug jeopardizing your confidential communications, or a hacked Facebook post, lawyers must stay conversant in and vigilant about the technology that impacts their practices.

About the Author

John G. Browning is a shareholder in the Dallas, Texas firm of Passman & Jones, P.C., where he handles civil litigation in state and federal courts, in areas ranging from employment and intellectual property to commercial cases and defense of products liability, professional liability, media law, and general negligence matters. Mr. Browning has extensive trial, appellate, and summary judgment experience and has represented companies in a wide variety of industries throughout Texas. Mr. Browning received his Bachelor of Arts with general and departmental honors from Rutgers University in 1986, where he was a National Merit Scholar and member of Phi Beta Kappa. He received his Juris Doctor from the University of Texas School of Law in 1989. 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 serves as Chair of the Texas Bar Journal Board of Editors, as a member of Professional Ethics Committee of the State Bar of Texas, and is a frequent speaker at CLE seminars and legal symposia all over the country.

The European ePrivacy Directive: The Companion to GDPR That You Need to Know

By Ronald Chichester

Along with the General Data Protection Regulation ("GDPR"),[1] there is a companion piece of EU legislation that is slated to come into effect in the near future. This companion piece is called the *ePrivacy Directive*.[2] The ePrivacy Directive was supposed to come into effect in May 2018, but that has been delayed until sometime in 2019.

The ePrivacy Directive, while being a companion to the GDPR, differs from the latter in significant ways. GDPR is all about *capturing* and *storing* data (at rest), while the ePrivacy Directive is designed primarily to protect that data while in transit.

But, the ePrivacy Directed covers a broader range of data than the GDPR. The GDPR is focused on privacy of the individual. The ePrivacy Directive includes non-personal data.[3] This difference has much to do with the difference in legal foundation between the two laws. The basis for the ePrivacy Directive are Article 16 and Article 114 of the Treaty on the Functioning of the European Union as well as Article 7 of the Charter of Fundamental Rights. The GDPR, on the other hand, is based on Article 8 of the European Charter of Human Rights, which is interpreted similarly to Article 7 of the Charter of Fundamental Rights.

As with GDPR, the ePrivacy Directive has some teeth in the remedies. Article 23 of the ePrivacy Directive allows administrative fines of up to EUR 10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[4]

Even though the penalties may seem onerous, the way to avoid them is simple: encrypt the data while it is in transit. You can send the data as an encrypted file, or transmit it by, for example, SSH or VPN on the Internet. These protocols are inexpensive (usually free) and easy to set up—and easier than inventing excuses.

---

[1] Regulation (EU) 2016/679, commonly known as the General Data Protection Regulation ("GDPR"). *See* Ronald Chichester, What's all the Fuss about GDPR, Cicuits Winter 2018, at 14.

[2] Regulation (EU) 2017/0003(COD), commonly known as the "ePrivacy Directive."

[3] *Id.* Explanatory Memorandum §§ 2.2, 3.1.

[4] *Id.* Art. 23.

About the Author

Ronald Chichester is a solo practitioner in Tomball who specializes in technology-related legal issues. He is past chair of both the Business Law Section and the Computer & Technology Section. Ron is a former adjunct professor at the University of Houston where he taught courses in computer crime and e-commerce. He is a registered patent attorney, a certified computer forensics examiner and a certified information systems auditor. Ron received his JD from the University of Houston and he holds a bachelor's and a master's degree (both) in aerospace engineering from the University of Michigan.

Information Quality Act Unlikely to Provide Cause of Action to Challenge the Accuracy of Information Distributed by Federal Agencies

By Ryan Gardner

At a time when numerous parties are searching for new and creative ways to challenge the actions of the Trump White House, some are invoking an obscure law known as the Information Quality Act ("IQA"), 44 U.S.C. § 3516 note, to challenge the administration's actions.[1] Passed as part of a 2001 appropriations bill, the IQA requires the Director of the Office of Management and Budget to issue guidelines to all federal agencies that "provide policy and procedural guidance to Federal agencies for ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by Federal agencies," and it specifies what the guidelines should contain.[2] Based on this stated purpose of ensuring the integrity of information released by federal agencies, plaintiffs are asserting the IQA gives members of the public a right to challenge what they consider to be inaccurate or misleading statements made by federal agencies. Even though these efforts are certainly a creative approach to challenge information distributed by the federal government, there is good reason to be skeptical that such lawsuits will succeed or even be allowed to proceed.

A quick review of the statute's text and case law reveals why. As explained by the Fourth Circuit Court of Appeals, the IQA merely "orders the Office of Management and Budget to draft guidelines concerning information quality and specifies what those guidelines should contain."[3] Nothing in the statute creates a legal right to access to information or to the correctness of that information. Thus, "almost every court that has addressed an [IQA] challenge has held that the statute creates no legal rights in any third parties."[4] Because no such legal right exists, courts have dismissed these types of claims. The justifications for such dismissals have varied slightly: some courts have held such plaintiffs lack Article III standing,[5] others have concluded plaintiffs may not use the IQA to challenge an agency's conclusions,[6] and still others have ruled an agency's refusal to correct distributed information does not constitute final agency action

---

1 Spencer S. Hsu, *Wielding obscure federal data quality law, group challenges Trump Treasury tax cut claims*, WASHINGTON POST (Nov. 14, 2017).

2 44 U.S.C. § 3516 note.

3 *Salt Institute v. Leavitt*, 440 F.3d 156, 158–59 (4th Cir. 2006).

4 *Miss. Comm'n on Envtl. Quality v. EPA*, 790 F.3d 138, 184 (D.C. Cir. 2015).

5 *Salt Institute*, 440 F.3d at 158–59.

6 *Miss. Comm'n*, 790 F.3d at 184–85.

subject to judicial review.[7] But the ultimate result remains the same, and such cases are not permitted to proceed.

Based on both the statute's text and the uniform way it has been interpreted by courts, judges are likely to view any lawsuits brought pursuant to the IQA with great skepticism. It is certainly possible for a court to reach a different conclusion in the future, but the growing consensus on this issue suggests such an outcome is unlikely.

About the Author

Ryan Gardner is an Associate in in Haynes and Boone, LLP's Business Litigation practice group in Dallas. His practice focuses on both appellate and trial matters. He holds a J.D. from Pepperdine University School of Law and was admitted to the Texas State Bar in 2016.

[7] *See Harkonen v. U.S. Dept. of Justice*, C 12-629 CW, 2012 WL 6019571, at *11 (N.D. Cal. Dec. 3, 2012) (collecting cases).

Cell phone text messages are discoverable—just not necessarily from the cell phone owner's employer

By Pierre Grosdidier

In a win for privacy, the Fourteenth Court of Appeals held in *In re Sun Coast* that a company could not be compelled to produce the work-related text messages on its employees' personal cell phones, even if the company partially paid for the service fees.[1] In the underlying wrongful death suit, the plaintiffs sought, *inter alia*, text messages exchanged between Sun Coast employees following a lethal gasoline explosion. The trial court issued an order compelling production of the text messages, but Sun Coast filed a petition for writ of mandamus wherein it argued that its employees' cell phones were not within its "possession, custody, or control and, therefore, [it could not] be compelled to produce any responsive text messages."[2] The court of appeals agreed and held that plaintiffs could instead obtain the text messages directly from the employees.[3]

That text messages are communications and are, as such, discoverable is undisputed.[4] But, the text messages in this case resided on the employees' personal cell phones. The plaintiffs argued that Sun Coast had "constructive possession" of the messages because the company handbook gave Sun Coast the right to inspect the phones to remove company confidential information. Moreover, Sun Coast employees used their phones for work and the company paid for part of the phones' service fees.[5] The court of appeals squarely rejected these arguments.

Analyzing the issues from a property right standpoint, the court held that cell phone owners "generally have the right to possess the device itself and to exclude others from the content of text messages stored on the device." Nothing in the at-will employer-employee relationship altered the parties' rights of possession and could allow Sun Coast to claim a superior right to the text messages. Moreover, the company handbook's policy was of no help because the text messages did not qualify as company confidential information. Finally, the fact that Sun Coast

---

1 *In re Sun Coast Res., Inc.*, 562 S.W.3d 138, 161 (Tex. App.—Houston [14th Dist.] 2018, orig. proceeding).

2 *Id.* at 156.

3 *Id.* at 160.

4 *See*, *e.g.*, Family Wireless #1, LLC v. Auto. Techs., Inc., No. 3:15-CV-01310(JCH), 2016 WL 3911870, at *4 (D. Conn. July 15, 2016) (absent objection, "text messages containing responsive information are discoverable.").

5 *In re Sun Coast*, 562 S.W.3d at 157.

paid for part of the phone's service fee was, absent details regarding the purpose of the reimbursement, insufficient to grant the company a possessory right in the text messages.[6]

The court cited to several federal district court cases that reached the same conclusion. It noted, however, that its holding applied to a private employment relationship and not a public one. In the latter case, text messages would be discoverable under the Texas Public Information Act.[7]

About the Author

Pierre Grosdidier is Counsel in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. Pierre divides his practice between construction litigation and construction contract drafting. He belongs to the first group of attorneys board certified in construction law by the Texas Board of Legal Specialization in 2017. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, a registered P.E. in Texas (inactive), and the State Bar of Texas Computer & Technology Section Webmaster and Circuits eJournal Co-Editor for 2018–19.

[6] *Id.* at 158–59.

[7] *Id.* at 160 n.17.

The REAL ID Act and its Implications for Texas Residents

By Sanjeev Kumar

The REAL ID Act is a federal law passed by Congress after 9/11 that established specific federal requirements for state-issued Driver License and Identity Cards to be accepted for certain federal purposes, like entering a federal building or boarding a domestic flight. The Act established minimum security standards for state-issued driver's licenses and identification cards and prohibits federal agencies from accepting for official purposes licenses and identification cards from states that do not meet these standards. Although passed in 2005, the Act will not fully go into effect until 2020. Starting on October 1, 2020, holders of non-compliant driver's licenses will not be able to use them as a form of identification to board domestic flights or pass through a TSA checkpoint.

State of Texas has submitted a plan to the Department of Homeland Security ("DHS") and as a result is now compliant with REAL ID law requirement, but the multitude of Driver's Licenses issued by the state are still not compliant with REAL ID. Under the plan submitted to DHS, Texas Department of Public Safety ("DPS") will issue REAL ID compliant driver's licenses and identification cards: REAL ID DL and ID Cards. These cards will be marked with a star and their holders will be able to use them as the sole form of identification for boarding domestic flights and entering federal buildings. All Texas driver's licenses cards and identification cards are currently acceptable to use for REAL ID purposes and Texans can use these documents until the earlier of their expiry date and October 1, 2020. But, in order to avoid any unpleasant experience after October 1, 2020, Texas residents should obtain a REAL ID compliant driver's licenses in the near future, even if their current card does not expire until a later date.

REAL ID-compliant driver's licenses can be obtained by visiting a DPS Driver License office with proof of identity, state residency, U.S. citizenship, or lawful presence in the U.S. The cost of REAL ID compliant cards is expected to remain the same as the current cost for a driver's licenses or identification card. Texas residents holding a non-compliant card after October 1, 2020 will not be able to board domestic flights or access federal buildings without secondary proof of identification approved by DHS.

The Act does not require individuals to present identification where it is not currently required to access a federal facility (such as to enter the public areas of the Smithsonian) nor does it prohibit an agency from accepting other forms of identity documents other than documents from non-compliant states (such as a U.S. passport or passport card). The Act's prohibitions

also do not affect other uses of non-compliant driver's licenses or identification cards for purposes unrelated to official purposes as defined in the Act.

About the Author

Sanjeev Kumar is the founder and principal at Hunt Pennington Kumar & Dula PLLC, which provides a wide range of legal services to entrepreneurs and business owners in the areas of business and corporate law and intellectual property. Sanjeev brings a vast wealth of experience in the tech industry to the table. Prior to practicing law, Sanjeev co-founded Portal Player, a semiconductor startup, and grew it into a NASDAQ listed company that was responsible for integral portions of the first seven generations of Apple iPods. Sanjeev understands the issues faced by his clients as he has walked in their shoes. He has been a successful technology professional, entrepreneur and business leader managing teams that were culturally diverse and located in different geographic areas. His technology and engineering experience along with business know-how in dealing with customers, suppliers and partners all around the globe when combined with knowledge of law makes Sanjeev a valuable adviser to entrepreneurs, professional managers and business owners.

We are Earthbound Astronauts: Smart Phone Geolocation Evidence

By Craig Ball

I give dozens of talks each year on electronic evidence where I discuss geolocation data and its transformative potential as evidence in criminal prosecutions and civil litigation. Smart phones constantly track our movements using gyroscopes, accelerometers, global positioning features, geolocation apps, cell tower triangulation and three independent radio systems. Our steps are tallied, altitudes logged, and, for many, vital signs are monitored, too. We are earthbound astronauts, instrumented and coupled to sensors and telemetry as thoroughly as any who journey into space.

This state of affairs doesn't fully resonate with audiences until I guide them through their own phones, showing the level of detail with which movements are tracked. Some listeners boast that they've set their privacy settings to block geolocation. They're the ones most surprised to learn that, although they can disable their ability to see their own geolocation history and stop geolocation data from being shared with apps, they can't disable geolocation broadcasting and still have a functioning phone. Here's the bottom line: if a phone can operate as a phone, it must broadcast its geolocation coordinates with a precision of ten meters (~30 feet) or better.

When I broach geolocation data and see that look of "we already know this" creep across faces, that's when I ask for a show of hands of how many in the audience use iPhones. Nearly every hand shoots up. I then invite them to drill down in their phone's Settings with me to the Significant Locations logs. Surprisingly, most have never done so before and are shocked, even frightened, by the richness of detail in the data.

To try it on your iPhone; navigate through **Settings**> **Privacy**> **Location Service**> **System Services**> **Significant Locations.** Unless you've disabled your ability to see geolocation data, you'll arrive at the phone's History list setting out locales visited, and the number of sites gone to within those locales.

But, wait! There's more! Tap on one of the historic locations and you'll see an annotated map of the area with blue dots denoting prior stops. Below this information is a more detailed list of addresses and sites visited (restaurants, stores, schools, etc.) with the number of stops noted. Here's where it gets interesting (or creepy, depending on your point-of-view). Click on one of the listed sites or addresses to see a zoomed-in map with a listing of the time and duration of each visit logged along with the time and mode of travel getting there (*e.g.*, 10 min drive, 4 min walk). Again, most of my audiences haven't seen these logs before and a few fairly freak out when they see their worst Orwellian nightmares come true. That's when I remind the lawyers listening to change hats; "*Doff your privacy Panamas and don your factfinder fedoras!*" Geolocation histories aren't something to fear. They're *gifts*. It's *evidence*. Powerful, probative, precise evidence.

Well, maybe not terribly precise. On the iPhone, geolocation coordinates occasionally pair to sites not visited but nearby. My iPhone sometimes mistakes the popular *Atchafalaya* restaurant

for my New Orleans home, although Atchafalaya is around the corner. The geocoordinates are right, but the pairing's wrong. Harmless error for the most part, but a quirk worth recalling when challenging geolocation data in court.

In U.S. trial practice, the ability to discover electronically-stored information (ESI) is a function of its accessibility. Relevant ESI that's reasonably accessible must be preserved and produced when sought if not privileged from disclosure. But when we speak of "reasonable accessibility," is it measured from the perspective of the custodian of the data (who enjoys ready access to geolocation data) or from the standpoint of service providers tasked to collect and process ESI? A phone's user can reach their phone's geolocation history in a few clicks; but it's daunting for e-discovery service providers to obtain the geolocation history with anything like the ease they secure e-mail or documents.

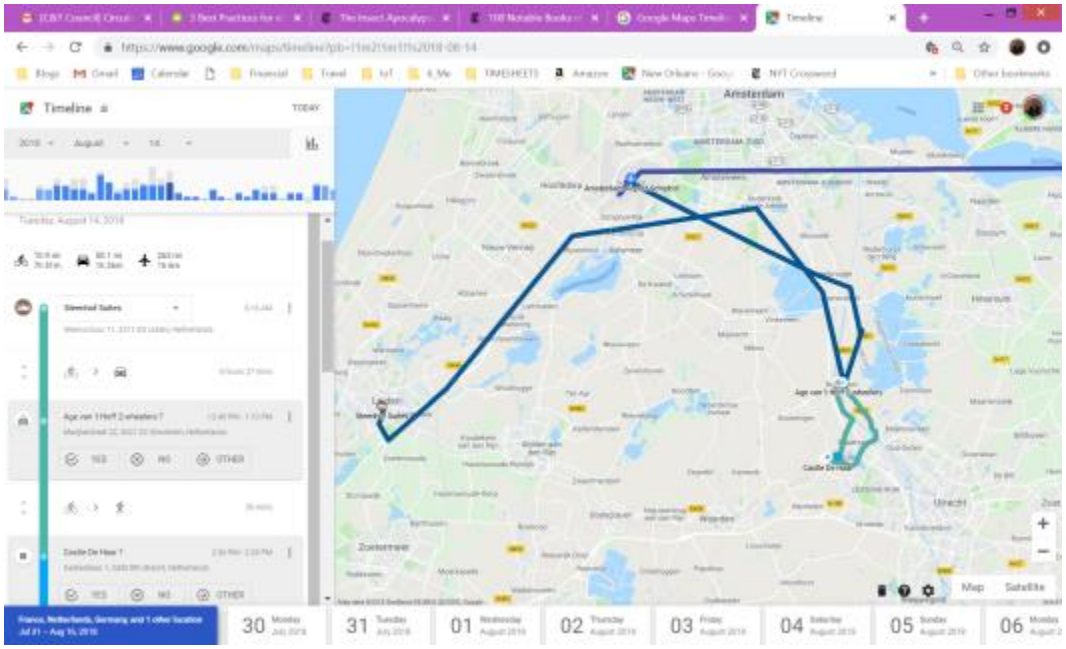
Apple doesn't permit geolocation coordinates to be stored in iTunes or iCloud backups, nor does Apple keep such data in its own records—so forget about serving a subpoena on Apple to get it. Excepting the geolocation data that U.S. laws require be shared with cell service providers to support 911 emergency services and the cell service provider's cell tower records, *a phone's geolocation history lives on the phone*. Accordingly, the "easiest" method of self-collection is also the most cumbersome and least searchable: grab screenshots of geolocation history screens.

Screenshots are a pain; but, all is not lost. An iPhone may be "jailbroken" by a forensic examiner and its geodata extracted. Else, the phone may have shared geolocation data with various apps serving as historical repositories.

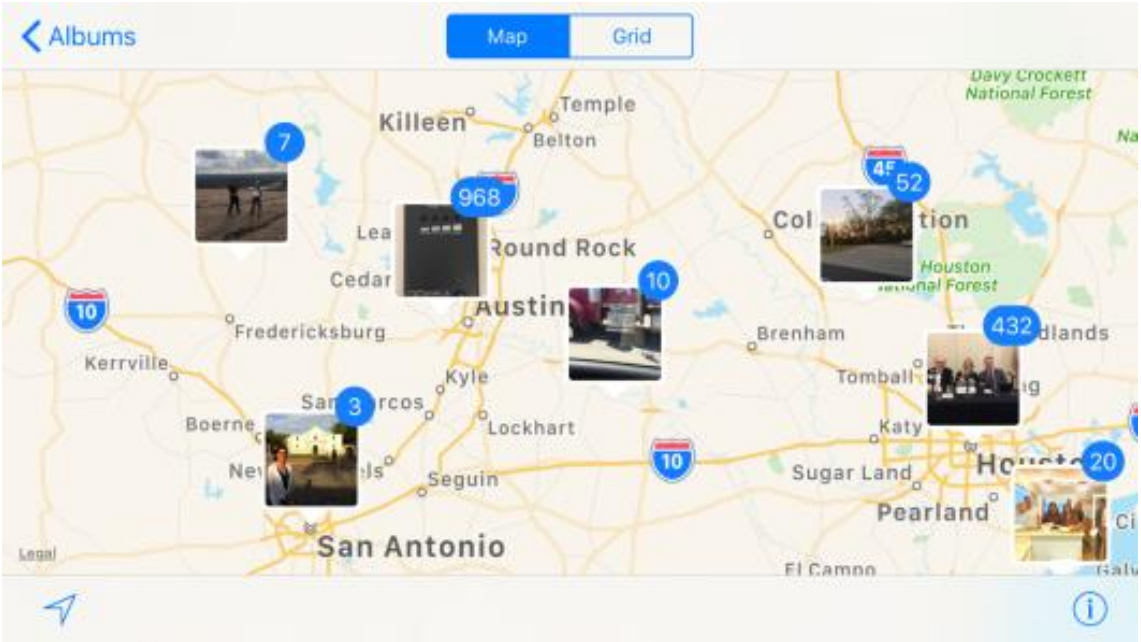
Two examples of application sources are Google Timeline (formerly Google Location History) and the geolocation data stored in photographs taken with the phone's camera. You won't have these sources in every matter because the former requires the user to have installed the Google Search app and granted the app access to geolocation data and the latter—though enabled by default—may have been disabled by a privacy-conscious user.

The geolocation data stored by Google Timeline is breathtakingly rich, reflecting place or business, arrival, departure, duration, route and mode of transport. The screenshot below depicts the data Google stored about my peripatetic wanderings for part of August 14, 2018. It starts at my hotel in Leiden, tracks my route by car, then bicycle rental, pedaling Utrecht, a visit to Castle De Haar and my evening flight from Amsterdam to Frankfurt. Google has been storing information about me with a comparable level of detail for at least five years. Happily for e-

discovery, Google allows users to freely and simply collect this data using Google Takeout (in JSON or KML formats). You can see your Google Timeline at google.com/maps/timeline and you can take out Location Services data at https://takeout.google.com.



The geolocation data that's embedded as EXIF data in smart phone photos includes precise longitude, latitude and altitude coordinates alongside information on date, time, phone used and more. An iPhone user can see their photos' geolocation mapped in **Photos**> **Albums**> **Places**> **Map** (screenshot below). As you pinch out, the precision boggles the mind. Mine shows which *room* in the house photos were made and extends back beyond eight years.



Can you imagine the power of robust geolocation histories to establish actions and interactions more precisely and reliably than fragile human memory? Consider the questions posed to U.S. Supreme Court nominee Brett Kavanaugh and Christine Blasey Ford in the confirmation hearings. Specific comings, goings, dates and places were forgotten or challenged; but today, would we have trouble proving teens were together? Probably not, because, today, everyone's a telemetered, terrestrial astronaut.

Isn't it time we put powerful, probative geolocation evidence to work for civil justice? It's right in the palms of our hands. When it's likely to be relevant, we should preserve it; moreover, we should take steps to insure our opponents preserve it. Screenshots of location histories aren't the best forms—they may be about the worst—but, screenshots aren't difficult or time consuming to create, and they're a darn sight better than preserving nothing at all.

About the Author

Craig Ball is a Board-certified trial lawyer who limits his practice to service as a court-appointed Special Master and consultant in computer forensics and electronic discovery. Craig teaches E-Discovery and Digital Evidence at the University of Texas Law School. For his articles on electronic discovery and computer forensics, please visit craigball.com or ballinyourcourt.com.

Don't Turn a Blind Eye to Dark Data: Part 1 – Image Formats

By Ronald Chichester

This is the first in a multi-part series about how to deal with "dark data"[1] in an inexpensive manner. Unfortunately, because most e-discovery tools skip over some uncommonly-formatted data (hence the term "dark data"), lawyers tend to skip dark data files and thus miss potentially important information. Dark data tend to be image files, video files, audio files, or just about anything that isn't an office document or email. Dealing with dark data is a common problem for litigators.

Image files often come in a wide variety of formats. For example, image files used for medical imaging are more often than not in a proprietary format that might be visible only with special software. Fortunately, in many cases, oddball images in oddball formats can be viewed with a simple open source[2] tool, which is thus free to download and use. That software tool is called Imagemagik.

Imagemagik can be used to view images in a wide variety of formats. More importantly, Imagemagik can be used to *convert* an image from its native format into another format that your e-discovery or other index tool can readily discern. Once converted, counsel should be able to view the image file in the normal manner. Alternatively, the attorney can use Imagemagik itself to display the image.

About the Author

Ronald Chichester is a solo practitioner in Tomball who specializes in technology-related legal issues. He is past chair of both the Business Law Section and the Computer & Technology Section. Ron is a former adjunct professor at the University of Houston where he taught courses in computer crime and e-commerce. He is a registered patent attorney, a certified computer forensics examiner and a certified information systems auditor. Ron received his JD from the University of Houston and he holds a bachelor's and a master's degree (both) in aerospace engineering from the University of Michigan.

---

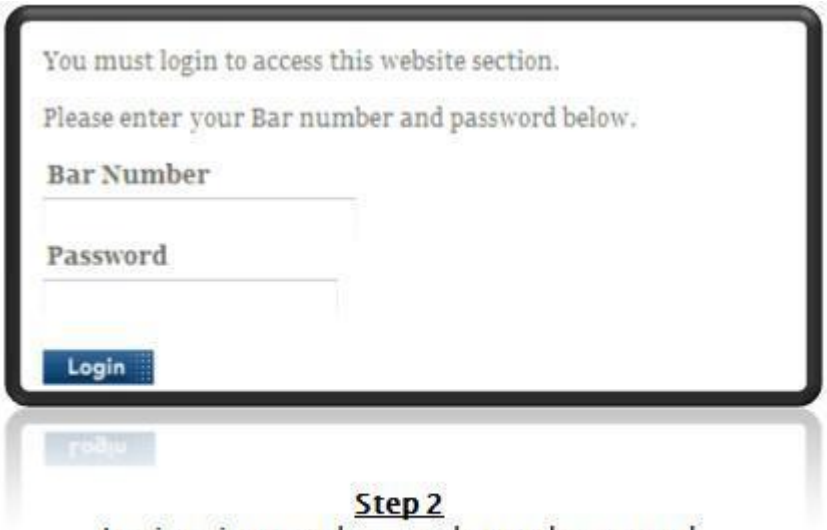
[1] "Dark Data" is defined as that data that, because of its storage format, remain opaque to most e-discovery or indexing tools. *See*, *e.g.*, Jackson Palmer, *Dark Data*, Inside eDiscovery, (September 28, 2015).

[2] Open source is a term meaning software that is provided under a license that adheres to the open source definition.

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

Sammy Ford IV – Houston – Chair
John Browning – Dallas – Chair-Elect
Shawn Tuma, Fort Worth – Treasurer
Elizabeth Rogers – Austin – Secretary
Michael Curran – Austin – Past Chair

Webmaster

Pierre Grosdidier – Houston

Circuits Co-Editors

Pierre Grosdidier – Houston
Kristen Knauf – Dallas/Fort Worth

Term Expiring 2021

Chris Krupa Downs – Plano
Seth Jaffe – Houston
Honorable Emily Miskel – Collin County
William Smith – Austin

Term Expiring 2020

Lisa Angelo – Houston
Eddie Block – Austin
Kristen Knauf – Dallas/Fort Worth
Rick Robertson – Plano

Term Expiring 2019

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

Chairs of the Computer & Technology Section

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