COMPUTER AND TECHNOLOGY SECTION

Circuits

e-Journal of the Computer & Technology Section
of the State Bar of Texas
December 2023

Table of Contents

Featured Articles

Short Circuits

Circuit Boards

Stay tuned for our FREE CLE each quarter!

Table of Contents

Circuit Boards:-

Letter from the Chair

By Reginald A. Hirsch

Holiday Greetings from the Computer & Technology Section! We thank you for being a member and please help us spread the word by urging your fellow colleagues to join as well.

Recently as Chair of our Section I attended the Council of Chairs, a bi-annual event hosted by our State Bar in Austin. This was a great event allowing the Chairs of the various Sections of the State Bar to personally interact with each other and share common issues and potential solutions. The State Bar provided up to date information regarding Bar activities and requirements for Sections per our State Bar rules and regulations.

On December 1, 2023 our Sections sponsored its 7th Annual Technology and Justice for All CLE live in Austin, Texas at the State Bar Building. This year's presentations were outstanding, and we thank our great presenters and our engaged audience for their participation and presence. As many of you know we offer this CLE free to the legal aid lawyers who serve our community. This year we were able to record our program through the assistance of Texas Legal services Center and especially Bruce Bower and Melissa Deutsch their videographer. By recording our CLE we are now able to provide to the Legal Service Community an opportunity to view our CLE for those Legal Aid Lawyers who were unable to attend our live CLE in Austin. As a secondary benefit we will be able to provide you as members of the Computer and Technology Section access to the CLE on our website, https://sbot.org. Currently the recording is being edited and should be available in early 2024.

In the spirit of this holiday season, I want to express my thanks to the officers and council and ex-officio members of our Section. They continued work and relentless efforts on behalf of the Section make the "Magic Happen"! Behind the scenes the work of the Section appears effortless but without their support and guidance we would not be able to provide our services to you as Section members and to our State Bar. A special thanks also to our Administrative Assistant, Erica Anderson, who never fails to anticipate an issue and provides guidance to our Executive Committee and Council. Thank you, Erica.

I also want to thank the State Bar Sections Department who so ably support our Sections. As many of you who work with the State Bar and attend various CLEs throughout the State it requires an enormous effort to coordinate Section activities, publications, and programming. This year after many years of service to the State Bar, Tracy Nuckols. Tracy over the years has

provided many untold hours in support and guidance for our Section and we wish you well in your new future. Lyndsey Jackson is our new Sections Department Director, and we are excited to work with Lyndsey and her great team and we congratulate her and thank her as she continues to support our Sections. Also, I would like to thank Paul Burke and Jake Stoffle with the State Bar, who help make the "Magic Happen".

The December 2023 Issue of Circuits is an outstanding issue for our members. The variety of articles and material will reward our members with scholarly and practical articles to be utilized in their everyday practice. We have articles and tips including, AI Discovery Issues, 4th Amendment cases dealing with iPhones, 3rd Party Rights and DNA Consent, Kid influencers, Preparing and Responding to Cyber Incidents, ADR Technology, Presenting Science Evidence, and Review of State and Federal laws regarding Privacy, Security and Wiretapping. To our great authors we appreciate your contributions to Circuits and thank you.

I would like to thank Sally Pretorius our editor of Circuits and Katie Stahl, associate editor. You both knocked it out of the park.

This year the State Bar of Texas honored our Section with a request to take over the programming for the "Adaptable Lawyer Tract" held annually at the State Bar of Texas Annual Meeting. This year's meeting will be held at the Hilton Anatole Hotel in Dallas Texas on June 20-21,2024. The "Adaptable Lawyer" tract will be on June 20,2024 and will be a full day CLE. With the guidance of our CLE Chair, Grecia Martinez and our CLE subcommittee I can assure you that this will be an outstanding CLE and we look forward to seeing you at the Annual Meeting.

Cindy Tisdale, President of the State Bar of Texas in her recommendation to the State Bar was to create a Working Group, now a Taskforce to examine issues surrounding Artificial Intelligence (AI) and the Law and to make recommendations to the State Bar. Currently the Chair of this Taskforce is John Browning and several of the appointed members of this Section serve on the Taskforce. The issue of AI and the practice of law has and will be a continuing issue for lawyers currently and into the future. The Computer and Technology Section has and will continue to monitor, write, and speak on these issues. AI platforms like ChatGPT and others will need to be evaluated for transparency, accountability, and accuracy. As Texas lawyers we have an ethical obligation under our Professional Code of Conduct to maintain "technical proficiency". Our Section has and will continue to examine these issues regarding AI and its usage by lawyers and provide information, resources, and guidance. We as a Section

strive to assist Texas lawyers in maintaining their “technical proficiency” and to respond with knowledge and resources regarding these every evolving changes.

Finally, our behalf of the Section we wish you and your family the happiest of holidays and a happy New Year.

Reginald A. Hirsch
2023-2024 Chair
Computer & Technology Section
State Bar of Texas

COMPUTER AND TECHNOLOGY SECTION

Discovery Tips for Cases When AI is the Subject of Discovery

Ronald L. Chichester

Introduction

This article focuses on generative AI, a type of artificial intelligence (AI) that presents unique problems for litigators. The need for this paper arose because "[g]enerative AI has suddenly become a must-have technology for almost every company. ... GenAI can also create human-like recommendations, robust content, and valuable new features for digital products that can improve user experiences."[1] This means that GenAI is being used for making decisions that carry legal implications. "As generative AI enters the mainstream, each new day brings a new lawsuit."[2] Not only is GenAI used to create new content, but other types of AI are used to make decisions that were, in years past, within the sole purview of humans.[3] Because AI is all about scale, centralization, and speed, any bad decision-making by AI tends to have extraordinary scope – with equivalent scope in a subsequent lawsuit – which makes AI a subject of discovery.[4]

---

1 Paul Smith-Goodson, "*The Extraordinary Ubiquity of Generative AI And How Major Companies Are Using It*" (Forbes, July 21, 2023) available at: https://www.forbes.com/sites/moorinsights/2023/07/21/the-extraordinary-ubiquity-of-generative-ai-and-how-major-companies-are-using-it/?sh=775573812124 (last accessed on October 2, 2023).

2 Kyle Wiggers, "*The current legal cases against generative AI are just the beginning*" (TechCrunch, January 27, 2023) available at: https://techcrunch.com/2023/01/27/the-current-legal-cases-against-generative-ai-are-just-the-beginning/ (last accessed on October 2, 2023).

3 Eric Colson, "*What AI-Driven Decision Making Looks Like*" (Harvard Business Review, July 8, 2019) available at: https://hbr.org/2019/07/what-ai-driven-decision-making-looks-like (last accessed on October 2, 2023); Sukwong Choi, et al., "How Does AI Improve Human Decision-Making? Evidence from the AI-Powered Go Program" (MIT, July, 2021), available at: https://ide.mit.edu/wp-content/uploads/2021/09/SSRN-id3893835.pdf?x96981 (last accessed on October 2, 2023).

4 See, e.g., Lior, Anat (2020) "AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy," Mitchell Hamline Law Review: Vol. 46 : Iss. 5 , Article 2. Available at: https://open.mitchellhamline.edu/mhlr/vol46/iss5/2; Arkfeld, Michael "*A Call to Action: Litigating Artificial Intelligence Cases*" (ABA The Judges' Journal, February 3, 2020) available at: https://www.americanbar.org/groups/judicial/publications/judges_journal/2020/winter/a-call-action-litigating-and-judging-artificial-intelligence-cases/ (last accessed on October 2, 2023). *See also*, *In the Matter of Everalbum, Inc.,* FTC Matter 192 3172 (May 5, 2022), available at:

Purpose

This paper offers tips to the electronic discovery (e-discovery) practitioner regarding the preservation and the acquisition of artificial intelligence models in e-discovery. Specifically, this article supplies guidance for adding additional language to litigation hold notices, requests for production, and preservation requests that are tailored to artificial intelligence models that are ***time-sensitive***.

The Types of AI that Require Special Handling by Litigators.

a. Machine Learning is a Subset of Artificial Intelligence

Artificial intelligence is a broad category of computer science that encompasses many technologies. "Machine learning is one way to use AI. It was defined in the 1950s by AI pioneer Arthur Samuel as 'the field of study that gives computers the ability to learn without explicitly being programmed.'"[5] Algorithms[6] can be programmed explicitly. However, to be explicit, the programmer must first understand all the variables and the parameters to be modeled by the algorithm. That is fine for problems of little or moderate complexity, but

> "[I]n some cases, writing a program for the machine to follow is time-consuming or impossible, such as training a computer to recognize pictures of different people. While humans can do this task easily, it's difficult to tell a computer how to do it. Machine

---

https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3172-everalbum-inc-matter (last accessed on October 9, 2023) (Everalbum settled Federal Trade Commission allegations that it deceived consumers about its use of facial recognition technology and its retention of photos and videos of users who deactivated their accounts. The settlement order stipulated that Everalbum had to "delete or destroy any Affected Work Product" [the AI]); *In the Matter of Cambridge Analytica, LLC*, (FTC Matter 182 3107), available at: https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3107-cambridge-analytica-llc-matter (last accessed on October 9, 2023) (FTC alleged that the CEO and app developers "employed deceptive tactics to harvest and to use personal information from tens of millions of Facebook users for voter profiling and targeting." The final settlement included the deletion of the information.); Tonya Riley, "The FTC's biggest AI enforcement tool? Forcing companies to delete their algorithms" (Cyberscoop, July 5, 2023) available at: https://cyberscoop.com/ftc-algorithm-disgorgement-ai-regulation/ ("So far, the FTC has used this tool in five cases against tech companies dating back to 2019.").

[5] Sara Brown, "Machine learning, explained" (MIT Sloan, April 21, 2021) available at: https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained (last accessed on October 2, 2023).

[6] *See, e.g.,* Marek Kowalkiewicz, "How did we get here? The story of algorithms" (Towards Data Science, October 10, 2019) available at: https://towardsdatascience.com/how-did-we-get-here-the-story-of-algorithms-9ee186ba2a07 (last accessed on November 1, 2023).

> learning takes the approach of letting computers learn to program themselves through experience."[7]

It should be noted that, while the original scope of the word 'algorithm'[8] was limited to that which was known and generates reproduceable results, the current scope of the word "algorithm" has been expanded to encompass machine learning models, which are often opaque, non-determinate, and do not necessarily generate reproduceable results.[9] This is unfortunate, because laymen tend to refer to traditional algorithms and machine learning interchangeably leading to confusion with experts' use of the terms. In this paper, the author distinguishes between algorithms (where the underlying process is known and well defined) and machine learning models (where the model mimics a process that cannot be reduced to a traditional algorithm). This distinction has important implications for e-discovery because current practices in e-discovery relating to software focuses on algorithmic-based software, and not machine learning models.

b. Not All Machine Learning Models are Alike

Machine learning comes in three general types that focus on *how* the models learn, namely: supervised learning; unsupervised learning; and reinforcement learning. Both supervised and unsupervised learning models go through an initial learning process, after which the models remain mostly "static" and unchanging. For this article, however, we are concerned with machine learning (ML) models that employ reinforcement learning because they can change *after* the initial learning process, which means that they are *designed* to change their decision-making behavior over time.

> "In **reinforcement learning** the [machine learning] agent learns from a series of reinforcements – rewards and punishments. For example, the lack of a tip at the end of the journey gives the taxi agent an indication that it did something wrong. The two points for a win at the end of a chess game tells the agent it did something right. It is up

---

7 Brown*, supra,* note 6.

8 A standard definition of 'algorithm' is: "An algorithm is a sequence of instructions that a computer must perform to solve a well-defined problem. It essentially defines what the computer needs to do and how to do it. Algorithms can instruct a computer how to perform a calculation, process data, or make a decision." Kassiani Nikolopoulou, "*What is an Algorithm? | Definition & Examples*" (Scribbr, August 9, 2023) available at: https://www.scribbr.com/ai-tools/what-is-an-algorithm/ (last accessed on November 2, 2023).

9 *See, e.g.,* Hilke Schellman, THE ALGORITHM: HOW AI DECIDES WHO GETS HIRED, MONITORED, PROMOTED, AND FIRED AND WHY WE NEED TO FIGHT BACK NOW (January 2, 2024).

to the agent to decide which of the actions prior to the reinforcement were most responsible for it."[10] (emphasis in the original)

In some cases, the ML process is continuous.[11] Continuous learning is one of the characteristics of machine learning that has rather unique implications for E-discovery. For practitioners, the elements of machine learning that connote continuous learning are: "reinforcement machine learning"; "reinforcement learning"; and "continuous machine learning."[12] If your client's or opponent's AI has any of those elements, then copying and archiving the AI in question may be pivotal to your case. Why is this type of AI potentially pivotal to a case? Because the whole point of reinforcement learning models is that they make *decisions* on behalf of people or organizations. The decision to act (or not) that was made by the model may be an element that gave rise to a cause of action. Hence, discovery about the AI/ML model is probative, and replication of the output results with the original input data that gave rise to the cause of action can lead to evidence of liability.[13]

---

[10] Stuart J. Russell & Peter Norvig, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH (3rd Ed. 2015), p. 708.

[11] *See, e.g.,* "MLOps: Continuous delivery and automation pipelines in machine learning" (Google Cloud Architecture Center, last reviewed on May 18, 2023) available at: https://cloud.google.com/architecture/mlops-continuous-delivery-and-automation-pipelines-in-machine-learning (last accessed on October 2, 2023).

[12] *See, e.g.,* Yashaswi Nayak, "Continuous Machine Learning: An Introduction to CML", (Towards Data Science, March 29, 2022) available at: https://towardsdatascience.com/continuous-machine-learning-e1ffb847b8da (last accessed on October 11, 2023); "Reinforcement Learning: Definitions, Types, Approaches, Algorithms and Applications (EduShots, November 7, 2021) available at: https://www.edushots.com/Machine-Learning/reinforcement-learning-overview (last accessed on October 11, 2023).

[13] *See, e.g.,* Paul W. Grimm, Maura R. Grossman, and Gordon V. Cormack, Artificial Intelligence as Evidence, 19 NW. J. TECH. & INTELL. PROP. 9 (2021). https://scholarlycommons.law.northwestern.edu/njtip/vol19/iss1/2; Kaushik Mitra, "From Code to Court: Role of Source Code in Detecting the FTX Fraud" (UnitedLex.com), available at: https://unitedlex.com/insights/from-code-to-court-role-of-source-code-in-detecting-the-ftx-fraud/ (last visited on November 1, 2023). ("In the current digital world, where financial transactions are enveloped in layers of code, the integrity of the underlying code of financial platforms is often taken for granted. However, beneath the sleek User Interface (UI) of these platforms, lies a vast ocean of code that operates like the constitution of the platform, expected to uniformly govern every transaction, every trade, and every financial operation carried out on the platforms. The recent, high-profile case brought against FTX and Sam Bankman-Fried highlights that source code review can play a critical role in evidence detection in litigations in many diverse domains.").

c. *Why Discovery of AI is Handled Differently than Regular Software*

In the past, software programs were composed of one or more algorithms that did not change across different versions of the software. For each version, identical inputs generated identical outputs; so, all that was necessary to preserve and to produce during discovery was a copy of the original version of the algorithm-centric software program and perhaps the computer system requirements needed to run the software. The underlying presumption was a preserved *copy* of the software would produce results identical to those that produced the problem in the first place. While that was a reasonable assumption for algorithm-centric software, it is not a valid assumption for machine learning models.

In contrast to algorithm-centric software programs, each *instance*[14] of a machine learning-based software program (ML model) *learns* from its own unique set of experiences. Thus, over time, *different* instances of ML models may be *expected* to produce *different* results against the same input data. Because ML models improve with experience, *each instance* of the ML model may produce different results over time, even when supplied identical inputs *if the ML model gained a new set of experiences in the interim and morphed.* In other words, if the evidence in your case depends upon "interviewing"[15] the ML model at different times, you may be shocked to see different results despite using identical data. Moreover, ML models typically can't remember (and typically don't log) *how* they arrived at a particular decision, so that evidence is lost. Without that evidence, if the original ML model has "morphed" because it acquired new experience *after* the act that gave rise to the litigation, the litigator may be unable to duplicate the decision-making process that led to the cause of action. Note, absent logging or journaling, the "morphing" through the acquisition of experience ***permanently*** alters

---

[14] By "instance" I mean that a copy of the machine learning model that is running on some device. The point here is that each instance of a particular version of an algorithmic-centered software application is identical to every other copy of that that version of the application. However, machine learning code that is based on reinforced learning can act differently from every other copy of that model because models often undergo different experiences, and thus adapt differently from their brethren. For example, a software developer can produce a reinforcement learning model, and then generate three copies of that model. At the outset, each copy will behave much like the other copies. However, should one instance be given an experience that is not shared by other instances, then that first instance will evolve (and behave) differently than the other instances. How much differently is be a matter of degree. For litigation purposes, you should not assume that all copies of a machine learning model will produce the same results from the same input. They may, but not necessarily, and never to the level of algorithm-based software.

[15] By "interviewing" I mean having an expert input data to the archived ML model and record the output to determine if the ML model contributed to an element in the cause of action.

the original ML model. Thus, any hope that the subsequent interview would yield probative and dispositive results depends upon promptly securing a copy of that particular instance of the ML model. That is why the preservation of this type of ML is time-sensitive.

d. New Clauses That Will Need to be Included in a Litigation Hold Notice and Requests for Production

A "litigation hold notice" is the means by which attorneys instruct their clients to preserve specific data for potential litigation. The goal of the litigation hold notice is to inform a client that specific types or items of information, particularly Electronically Stored Information (ESI), must be preserved for anticipated litigation and requests for discovery. In the case of ML models, particularly ones that learn from experience, the preservation process is different than that applied to routine documents. Unlike standalone executables, the ML model is part of a larger ecosystem, as illustrated in Figure 1:

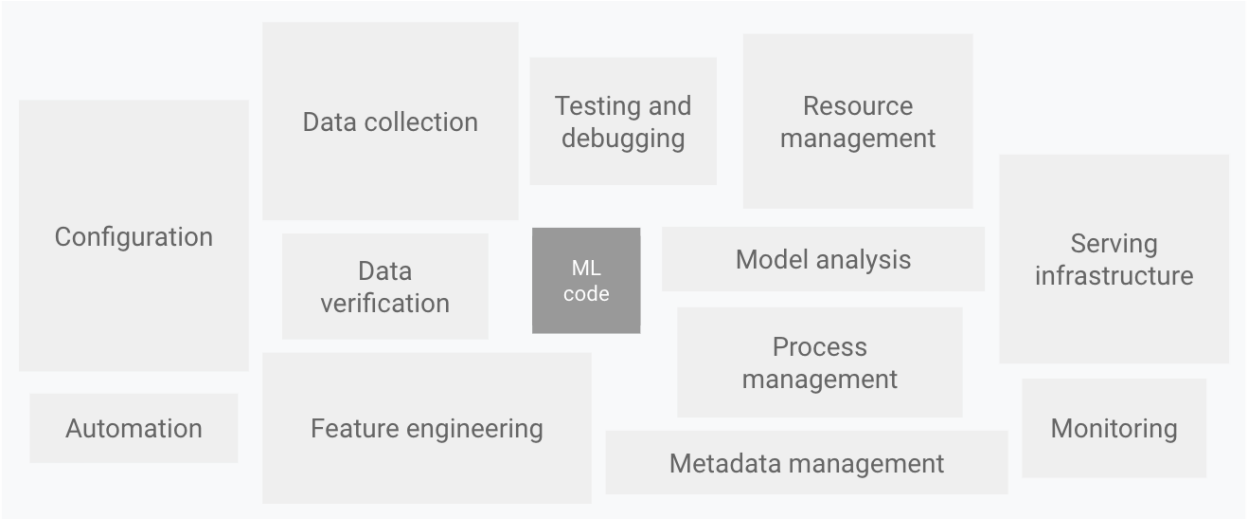


Figure 1: Elements of a Machine Learning Ecosystem[16]

For the ML model to run properly, and to be interviewed correctly for admissibility, ***all*** of the other code within the ML model's ecosystem must also be present and operational. Consequently, the entire ecosystem must be preserved. Note, normally the ML model's ecosystem sits within a single folder on a server's file system; however, other parts of the ML model's ecosystem may reside in other parts of the server's file system, or on separate

[16] *Id.* This chart was adapted from another article by D. Sculley, et al., "Hidden Technical Debt in Machine Learning Systems" (NeurIPS Proceedings, 2015) available at: https://proceedings.neurips.cc/paper_files/paper/2015/file/86df7dcfd896fcaf2674f757a2463eba-Paper.pdf (last accessed on October 3, 2023).

(remote) servers that may be in other jurisdictions. Drafting a litigation hold notice or request for production that calls for capture of only the ML model itself is unlikely to secure a working version of the ML model that an expert witness will require for the interview. Furthermore, *delays* in preserving the totality of the ecosystem serves to compound the problem because the ML model may be modified by new experiences in the interim, rendering them unable to replicate the processes underlying the cause of action. Courts may view such a failure to preserve replicability as a form of spoliation.[17]

While this paper offers specific warnings about certain types of AI, one seasoned veteran of the e-discovery world reminds us, "there is no perfect preservation letter."[18] That cautionary note is acutely applicable to machine learning ecosystems. Currently, attorneys must craft bespoke litigation hold notices and requests for production--a process often requiring the aid of experts. No one-size-fits-all litigation hold notice will suffice. Eventually, ML models will become commoditized--accessible to professionals and laypersons alike--such that e-discovery of those future models will become commonplace. For now, litigators will likely need to incorporate a clause in hold notices that supplies broad parameters for preservation sufficient to alert opponents to the necessity of preserving the ML model and its attendant ecosystem.

Unfortunately, a broadly-worded clause that would encompass a wide range of ML models and attendant ecosystems may draw objection as a "fishing expedition."[19] Such an objection would be unfounded: The "documents" that would need to be produced are computer files that, aside from running the ML model in question, pose no threat to the respondent and are relevant and responsive. The need for preservation of ML-related code (both script and binary) should be deemed proportional. Moreover, outside of the ML model, the software in the ecosystem is

---

17 *See*, *e.g.*, F.R.C.P. Rule 37(e); Paulette Kehely, "What Is Spoliation of Evidence, And How Can You Prevent It?" (DigitalWarRoom, March 19, 2020) available at: https://www.digitalwarroom.com/blog/what-is-digital-spoliation (last accessed on October 3, 2023).

18 Craig Ball, "The Perfect Preservation Letter: A New Guide" (Ball In Your Court, September 10, 2020), available at: https://craigball.net/2020/09/10/the-perfect-preservation-letter-a-new-guide/ (last accessed on October 3, 2023).

19 *See, e.g.,* David Horrigan, "e-Discovery Fishing Expeditions and the Mick Jagger Discovery Doctrine" (Relativity Blog, November 17, 2016) available at: https://www.relativity.com/blog/e-discovery-fishing-expeditions-and-the-mick-jagger-discovery-doctrine/ (last accessed on October 3, 2023); Mark Lanterman, "Proportionality and digital evidence" (Minnesota State Bar Association, 2019) available at: https://www.mnbar.org/resources/publications/bench-bar/columns/2019/11/04/proportionality-and-digital-evidence (last accessed on October 3, 2023).

non-prejudicial and is essential to the need for reproduction of the decision-making process by the ML model that is central to the cause of action.

e. The Rule 26(f) Conference – an opportunity to identify the AI early on

Rule 26(f) of the Federal Rules of Civil Procedure (FRCP) provides a framework for parties to discuss and to plan the discovery process in complex civil litigation. The purpose of the Rule 26(f) conference is to ensure that the parties have a clear understanding of the scope of discovery, the types of documents and information that will be exchanged, and the timeline for completion of discovery.

There are several key points about the content of the Rule 26(f) conference, namely:

1. Timing: The Rule 26(f) conference must take place within 21 days after the parties have been served with the complaint or notice of removal, whichever is earlier.
2. Participants: The conference is typically attended by the parties' lead counsel and any other persons who will be involved in the discovery process, such as designated discovery representatives or experts.
3. Agenda: The parties should prepare an agenda for the conference that includes the following topics:

    - Identification of the issues to be discovered
    - Definition of the scope of discovery
    - Identification of any electronic discovery (e-discovery) issues
    - Discussion of the methods and timelines for collection, processing, and review of discoverable information
    - Identification of any privileged or confidential information that may be relevant to the case
    - Proposals for the use of technology-assisted review (TAR) or other advanced search techniques

4. Preparation: Before the Rule 26(f) conference, the parties should review the pleadings and any relevant documents to identify potential areas of discovery. They should also consider the following:

    - Identifying key witnesses and their expected testimony
    - Determining the types of documents or information that may be relevant to the case

- Developing a plan for collecting, processing, and reviewing discoverable information

5. Outcomes: The Rule 26(f) conference can result in several outcomes, including:

    - A mutual understanding of the scope of discovery and the methods that will be used to collect and review discoverable information
    - Identification of any privileged or confidential information that may be relevant to the case
    - Agreement on a timeline for completion of discovery
    - Identification of any issues that need to be addressed through motions or other written submissions

6. Reporting: After the conference, the parties should prepare a written report that summarizes the discussions and agreements reached during the conference. The report should be filed with the court and provided to all parties.

Overall, the Rule 26(f) conference provides an opportunity for the parties to engage in early and extensive discovery planning, which can help to streamline the discovery process, reduce costs, and avoid potential litigation over discovery issues. However, while all of Rule 26 is relevant to AI/ML models, the most important issue for this article is *timing*. Because reinforcement learning models change over time (often well within the 21 days of serving the complaint) and because the attorney cannot delegate e-discovery to clients or non-lawyers,[20] it behooves the attorney to determine *well before the 26(f) Conference* whether or not machine learning models are relevant and, in particular, if those models rely upon reinforcement learning so that a copy of the model (and associated dependencies) can be preserved and produced. Quick action, and the documenting of the preservation scope and process for the reinforcement learning model, may preempt a motion for sanctions under Rule 37.[21]

Conclusion.

Artificial intelligence poses new challenges for litigators and in-house counsel alike. Simply knowing that AI or ML is involved with the cause of action should trigger an appropriate

---

[20] Federal Practice Committee of the U.S. District Court, District of Minnesota, *Discussion of Electronic Discovery at Rule 26(f) Conferences: A Guide for Practitioners* (January 2021) at 1, available at https://www.mnd.uscourts.gov/sites/mnd/files/eDiscovery-Guide.pdf (last accessed on November 1, 2023).

[21] Rule 37, Fed. R. Civ. P.

litigation hold notice and inform the scope of Rule 26(f) conferences and subsequent requests for production. In some cases, there may be a small window of opportunity to preserve the ML model adequately, making the urgency for preservation a crucial factor.

About the Author

Ronald L. Chichester is an attorney, AI engineer, legal engineer, expert witness, patent attorney, computer forensic examiner, and former adjunct professor of law who has taught courses in electronic discovery, computer forensics, intellectual property, and computer crimes. B.S. Aerospace Engineering, University of Michigan; M.S. Aerospace Engineering, University of Michigan; J.D. University of Houston Law Center. Former Chair of the Business Law Section and the Computer & Technology Section of the State Bar of Texas.

Science Needs a Story

By Robert G. Smith

Why Storytelling is Important for Technical Information

Despite how clear you believe your expert's opinions are, how irrefutable the numbers are, technical evidence does not sell itself. Many people do not understand how to interpret scientific or technical information and some people, today more than ever, are even suspicious of technical information.

Most people do not process abstract concepts very well, but they do tend to empathize with others who share similar interests and experiences. It is critical to know your audience (*i.e.*, the jury, judge, or the witness) as humans and speak to them with human stories and incorporate the science or technical information to support parts of the story.

Decisions are often based on emotion rather than logic. Emotion is important in helping us make timely decisions. Neuroscience research has shown that people who have brain damage in the area that helps process emotions have difficulty making decisions such as choosing a restaurant. Their decision-making skills are impaired due to lack of emotional judgment. Telling a story with technical information involves a combination of data, visuals, and narrative. When you combine these elements correctly, you have a story that can influence the emotion of your audience.

Use technical information to support your narrative that reinforces shared values among your audience members. Do not assume that because data supports a particular conclusion that your audience will reach the conclusion without a familiar narrative that resonates with personal experience. It is not enough that scientific data support a particular element of your story, the story should explain why the concept is believable on a human level. What conclusion does the data support and how does it fit into the context of the position you advocate?

Creating Compelling Stories

Storytelling means structuring your ideas properly to convey your intended message. Using technical information requires balancing telling a story with a clear message and logical sequence that is adapted to the audience with the help of detailed statistics or science that gives in-depth analysis or scientific support.

1. *Define your goal*

Begin constructing your story by determining what specific question you are trying to answer (a particular question in a jury charge), the goal you want to reach (a negative finding on a liability question), and how your expert information or scientific data is relevant to answering the question or reaching your goal.

2. *Simplify*

Break down technical concepts into pieces that can be explained to a young child. Use simple language and avoid technical terminology as much as possible. The more technical terms you have to define and that your audience must remember, the more difficult it is to follow your story. Using clear, simple language does not mean you cannot communicate difficult ideas. You can build a technical story by creating a narrative one simple idea at a time. Remember that our ability to comprehend technical information has not progressed as quickly as innovation itself.

If statistics are helpful to your story, create a visual exhibit or a colorful graph or chart, rather than just a list of numbers. Explain what the parts of the graph mean in simple terms so that your jurors or other audience will be able to refer to the infographic and advocate your position to each other during deliberations.

You can get ideas about how to create simpler stories from technical information by searching for "your keyword" plus "explain to a 5-year-old."[1]. You will find examples of how to simplify most anything.

3. *Techniques*

Developing a compelling story using technical information helps make the information more memorable, more persuasive, and more engaging for the audience.

A deliberate way to start building a compelling story is to use a formal storytelling structure such as Freytag's Pyramid which can help ensure that you include the necessary elements for a complete narrative. Freytag's Pyramid is a structure for dramatic storytelling that includes the following five elements:

a. Exposition
b. Rising action
c. Climax

[1] 5 Storytelling Ideas for your Next Technical Presentation, Valdas Maksinavicius, November 13, 2016.

d. Falling action
e. Catastrophe or resolution

Once you have created a compelling narrative, you can reference technical information at critical points along the story line.

Consider the age, demographics, background of the audience. For example, a jury with multiple engineers may appreciate more lists of numbers or graphs than a jury with people from less technical backgrounds. It is not enough to simply explain the data shown by graphs or technical diagrams. It is critical to connect the data to the story you are telling and discuss how the data supports the storyline and resolution to the problem. Doing so creates buy-in from your audience and encourages them to reach your conclusion.

Reuse Familiar Stories

Use familiar examples to help make concepts more understandable and relatable. While outside counsel and the client may spend two or more years working on a case and develop intimate knowledge about the subject (the product, process, market, accident, transaction, etc.), jurors and the judge only have a short time to learn about your case and why your position is correct.

Using familiar story lines like those found in fairy tales, movies, or popular books or games, help create immediate connection with your audience. A familiar story accelerates the process because jurors are already familiar with your story which you can adapt to your narrative and use technical evidence (expert testimony, literature, testing, etc.) to buttress points in your narrative that support elements of your claim or defense.

Your audience will not be familiar with materials science, but they know The Three Little Pigs, a fable about three pigs who build three houses of different materials. Think of your narrative as building a house. Each part of your story is a brick, but the science and technical information is the mortar that you put around the bricks to build a solid structured narrative. Make sure to explain the context of the scientific information and why it is important to helping your audience reach your intended conclusion.

Maximize Credibility

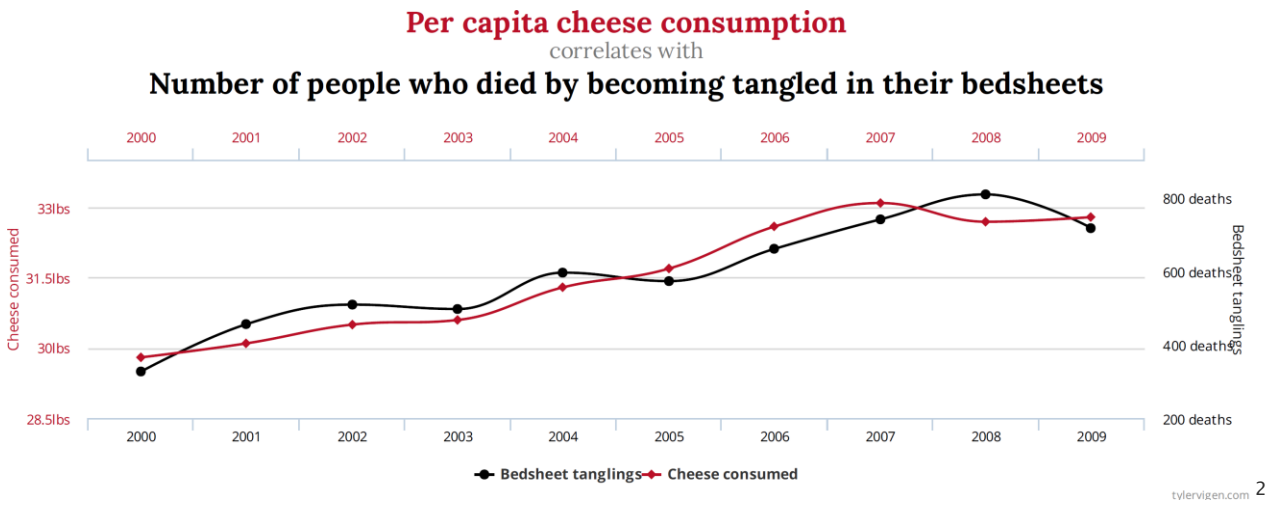
Walter Fisher, an American academic who developed narrative theory, suggested that all communication happens through narratives, symbolic interpretations of the world that connect with particular times and places, and it is more important how stories are interpreted and believed than whether they include scientific truth. It is easy for an audience to believe a story

that is coherent and consistent even if it is not true. Rumors spread easily when the story follows a familiar narrative and includes simple arguments that resonate with the audience but such a rumor can include lies and stereotypes that are harmful.

Your narrative is stronger when your technical information is more credible. Strategies to maximize the credibility of your technical data include:

a. Disclose potential biases in the data that you use in your story because you can be certain that the opposing party will do so. Being the first to share bias or potential flaws in data analysis helps humanize the data and connect with your audience. Showing vulnerability in your narrative is important to connect the speaker to the audience.
b. Do not manipulate the scale of data when selecting the units of measurement. Doing so can make statistics or other data compelling, but it may create a false representation that will be easily attacked.
c. Do not cherry pick only specific data points that support your ideas if there is as much or more data that contradicts your idea.
d. Be consistent with visual representations of data, such as consistent colors, labels, and naming conventions, which creates cohesiveness in your storytelling.
e. Statistics and other data can be manipulated to support alternative positions, which is why it is all the more important to break it down as simply as possible, to help avoid confirmation bias.

When your opponent fails to do any of these things, highlight such inconsistencies or inaccuracies for the jury during cross-examination or elsewhere. For example, a concept that often comes up with experts is the difference between correlation and causation. Correlation refers to the degree of association between two variables, how closely they resemble one another. Positive correlation is when A increases B also increases, or if A decreases then B decreases. Negative correlation is when A increases then B decreases and vice versa. However, correlation does not suggest A caused B or B caused A. Sometimes it is just a coincidence. For example:



Of course, eating more cheese does not cause you to be more likely to die from bedsheet entanglement. Be on the lookout for such spurious arguments from experts or misrepresentations in material presented as technical "evidence."

Sometimes it is necessary to use scientific data to meet a legal standard of proof or because your audience requires it. Use the necessary technical information to support points of your narrative to help connect the hearts and minds of your audience. Data usually explain the "what," which jurors may understand in their minds but you must develop a compelling narrative to connect the data to the "why" if you want to also reach their hearts. If you apply mortar (your narrative) to the bricks (scientific evidence) appropriately, then the wolf (opposing counsel) will not be able to blow your house down.

[2] Spurious Correlations, www.tylervigen.com.

About the Author

Robert G. Smith is a capable litigator and is a partner in Mayer LLP's Houston office. Rob was the Chair of the Medical Defense & Health Law Committee in the International Association of Defense Counsel (2021–2023), and he is also a member of the IADC Product Liability and Business Litigation Committees. Rob is on the steering committee of the ALFA International Product Liability & Complex Torts Practice Group and is a member of the Business Litigation and Corporate Transactions Practice Groups. Rob graduated Phi Beta Kappa with a degree in mathematics from Louisiana State University and attended law school at University of Houston Law Center. He is Board Certified in Personal Injury Trial Law by the Texas Board of Legal Specialization and has tried a wide variety of cases during his 27+ years of practice. He can be reached at rsmith@mayerllp.com.

Law Firms in the Crosshairs: Preparing for and Responding to Cybersecurity Incidents

By Candace McCaddon

Cyber-attacks targeting law firms are skyrocketing, with three of the top firms-- Kirkland & Ellis, K&L Gates, and Proskauer Rose—falling victim just this year.[1] And it is not just large firms falling victim. According to the American Bar Association's 2022 Legal Technology Survey Report, 27% of law firms reported having experienced a security breach at some point.[2]

Law firms hold a treasure trove of financial information, intellectual property, and other confidential and personal data of their clients. Coupled with the fact that they commonly lack dedicated cybersecurity resources, it is easy to see why law firms are prime targets for hackers.

The consequences of an incident can be severe. The global average cost of a data breach is now $4.45 million, with professional services firms bearing an even higher average cost of $4.47 million according to IBM.[3] In addition to the direct costs of responding to and recovering from an incident, firms face potentially significant third-party liability. Increasingly, this third-party liability includes class action lawsuits contending that the firm had failed to adequately secure its network and to protect sensitive client data.

Cyber-criminals can target a law firm's IT infrastructure in many ways, including exploiting vulnerabilities associated with email and email servers, phishing scams, Wi-Fi network access point attacks, and breaches that deploy ransomware on computers and data servers, for example. Personal devices, including mobile phones, desktops, laptops, and other devices, are just some examples of potential attack vectors. Law firms can no longer ignore the growing cybersecurity threat. The goal of this article is to share how law firms can prepare for, respond to, and mitigate the impact of cyber incidents.

---

1 Staci Zaretsky, Top Biglaw Firms Targeted In Global Cyber Attack, Above the Law (Jul. 6, 2023, 12:12 PM), https://abovethelaw.com/2023/07/top-biglaw-firms-targeted-in-global-cyberattack/.

2 2022 ABA Legal Technology Survey Report, American Bar Association (Nov. 29, 2022), https://www.americanbar.org/groups/law_practice/resources/tech-report/2022/cybersecurity/.

3 Cost of a Data Breach Report 2023, IBM Security (Jul. 2023), https://www.ibm.com/downloads/cas/E3G5JMBP.

Key Steps to Reduce the Risk and Potential Impact of a Cyber Incident

No law firm can protect itself completely from the possibility of falling victim to a cyber-attack. However, strategic investments of its time and money can greatly reduce the potential impact of an inevitable breach. The most notable mitigants include procuring cybersecurity insurance, implementing and maintaining good security tools and practices, and preparing and practicing an incident response plan.

Cybersecurity insurance provides critical financial resources, and potentially support services, when a firm is attacked. Legal professional liability coverage, *i.e.*, malpractice insurance, does not offer the same coverage as cyber insurance and relying solely upon malpractice insurance can leave a law firm exposed. Cyber policies may cover costs associated with liability to third parties or direct expenses, such as:

- ransom payments necessary to restore access to data or to prevent hackers from releasing stolen confidential information,
- costs to restore data from back-ups should the law firm choose not to pay ransom,
- costs to hire experts, including computer forensics to uncover the source and extent of an attack,
- notification costs,
- loss of income due to business interruption,
- costs associated with remediating and restoring a law firm's network,
- costs associated with losses due to theft, and
- costs for regulatory fines.

The underwriting process for cyber insurance typically requires proof that a law firm currently implements and maintains adequate security controls. If a law firm has not thoroughly addressed information security, or if it lacks critical security controls, it may affect the cost of, or the ability to acquire cyber insurance. Regardless of the size of a law firm, there are basic security practices it can implement, which are critical to protecting its data.

Fundamental security controls include:

- creating and implementing a data security policy,
- training all law firm employees on best data security practices on a regular basis,
- using complex passwords that are at least 12-14 characters long and changing them regularly,
- using multifactor authentication,

- encrypting sensitive data at rest and in transit,
- implementing access control to allow individuals access only to that information which they need to know,
- using only secure mobile applications,
- evaluating the security practices of its vendors,
- creating and testing an incident response plan (including a communications plan), and
- backing up the law firm's data to secure servers and including data recovery in its incident response plan.

Small and medium sized law firms typically do not have dedicated IT staff, let alone cybersecurity professionals. There are many managed security services providers that can fill the gap by offering a suite of services and tools to bring a law firm's cybersecurity hygiene up to par at affordable prices .

The importance of developing and practicing an incident response plan (IRP) cannot be overstated. An IRP should include assigning roles and responsibilities to certain individuals, along with their up-to-date contact information (including information on how to contact them after hours). Technical protocols and escalation points should be outlined, and the IRP should include a plan for resource gathering and documentation.

A communications plan is a critical part of an IRP, especially as it pertains to communicating to a law firm's partners, employees, and clients during a crisis. It is prudent to prepare out of band methods of communication in the event a law firm's entire network must be taken offline or the security of existing methods of communication is called into question otherwise.

Equally as important is including potential notification triggers and regulatory requirements, so a law firm minimizes the amount of time it spends scrambling mid-incident. Last, but not least, a law firm should establish an IRP review and testing schedule, so the IRP is kept up-to-date and rehearsed.

Keep in mind that a cyber insurer may have very specific requirements to support a claim. A policy may contain claim notification clauses with strict timeframes to report incidents – often 48-72 hours. An insurer may mandate certain response activities or the use of specific vendors, too. Insurers will require detailed accounting of the response and recovery expenses and labor costs. A law firm will need to keep thorough records. Records of lost billings, contractual fines, consulting fees, and other breach-related costs all need to be captured.

With these foundational elements in place, law firms can minimize damage and have faster recovery time if and when a cybersecurity breach does occur.

Time is Money: Executing the Incident Response Plan

> "Time is the new currency in cybersecurity, both for the defenders and the attackers. . . early detection and fast response can significantly reduce the impact of a breach"
>
> – Chris McCurdy, GM Worldwide IBM Security Services.

One of the hardest parts of incident response is detecting if an incident occurred in the first place. Often, the first indication may be a frozen device with a message from an attacker or other notification directly from an attacker alerting the user to an incident (imagine receiving an email from an anonymous source with evidence showing that the person has access to confidential client information).

If a cyber-attack is detected, activating the incident response team quickly per established protocols is key. Immediate containment and isolation are critical, as is notifying a law firm's key internal contacts and insurers.

The next priority is to determine the source and scope of the impact. A forensic investigation can reveal how, and which systems and data have been compromised. Regardless of whether a law firm has internal forensics experts, it may be prudent to hire an independent third-party company specializing in cybersecurity incident response to conduct a forensic investigation to best position the law firm to defend itself against any subsequent third-party claims and liability.

If a law firm is experiencing a ransomware attack, it may be wise to engage an outfit specializing in ransomware gang negotiations if for no other purpose than to buy time to recover its data from back-ups.

Next, the law firm needs to think about mandatory notification and reporting obligations. Is the law firm subject to any mandatory reporting obligations under any regulatory regimes, breach notification laws, contracts, or otherwise?

Controlling the narrative during incident response is of paramount importance, too. Strategic communications are key. A law firm will want to notify its partners, employees, and clients as soon as practicably possible. The last thing a law firm wants is for its employees and clients to learn about the breach from the media or from third parties. Careful communications that

avoid conclusory or premature statements, but that strike a balance with transparency, are key in this regard.

And how will the law firm's attorneys continue to communicate and work? If the incident response team switched to out of band communications due to network outages or other impacts of the incident, it must ensure its attorneys are not using unsanctioned personal email. And, if a law firm decides to let employees use personal accounts or out of band communications, it must be sure to establish clear, easy to follow rules and to communicate to clients ahead of time how it is maintaining the security and confidentiality of clients' information.

While attacks can and will happen to law firms of all sizes and levels of sophistication, preparation and planning equip law firms to respond quickly to minimize damages by leveraging every resource available to respond as quickly and seamlessly as possible.

About the Author

Candace McCaddon has over 15 years' experience helping clients with technology transactions, as well as information security, intellectual property, and privacy matters. After spending a decade in-house at various Fortune 100 companies in the energy, chemical, and engineering and construction industries, she launched her own practice in 2023. Her clients include some of the largest global engineering and construction companies in the world, as well as small and mid-sized managed cybersecurity services providers.

State & Federal Legislation for Data Privacy and Security

By Kellye Hughes

Texas recently enacted legislation to protect the privacy and security of individuals who provide their personal, identifying information to offline and online businesses. The legislation, Texas Data Privacy and Security Act (TDPSA) allows several businesses and entities exemption from compliance with the Act. The Act's intended purpose is to allow individual consumers to opt out of having personal data used or sold to third parties. The legislation funded attorney and staff positions in the Texas Attorney General's Office to monitor and enforce violations of this Act.

The U.S. Congress is on its second attempt to establish similar, but more comprehensive legislation, the Federal Online Privacy Act of 2023 (OPA). The OPA would create a Federal Agency to enforce the legislation and would allow state's Attorney Generals to monitor and enforce violations of the Act. Under the OPA, entities excluded from compliance under the TDPSA would be required to comply with the privacy legislation.

Texas Data Privacy and Security Act

On June 19, 2023, Texas Governor, Greg Abbot, signed the Texas Data Privacy and Security Act. Texas is the sixth state to pass a comprehensive data privacy law this year. The Act will take effect on July 1, 2024. The Act was sponsored by Texas State Senator Bryan Hughes (R) and co-authored by Rep. Giovanni Capriglione (R), Rep. Oscar Lee Longoria Jr. (D), Rep. Dustin Burrows (R), and Rep. Morgan Meyer (R). The bill required ten votes prior to passing.

The bill amends the Business & Commerce Code by adding Chapter 541, The Texas Data Privacy and Security Act (TDPSA), addresses the regulation of the collection, use, processing, and treatment of consumers' personal data by certain business entities. TDPSA provides consumers residing in Texas with certain rights regarding personal data. Protections include: the right to request confirmation of whether a controller is processing the consumer's personal data; the right to correct inaccuracies in personal data; the right to delete personal data provided by or obtained about the consumer; the right to obtain data (if feasible) in a portable, readily usable format so that the consumer may transmit it to another controller; and the right to opt out of the processing of personal data for purposes of targeted advertising, sale of personal data, or profiling. The Act applies to a person or entity that conducts business in Texas or produces products or services consumed by Texas residents and processes or engages in the sale of personal data.

The scope of the Act excludes a small business as defined by the United States Small Business Administration, except with respect to the provision that requires small businesses to obtain consumer consent prior to selling sensitive data. The Act also does not apply to State agencies or political subdivision, financial institutions, entities governed by the United States Department of Health and Human Services, non-profit organizations, institutions of higher education, and electric providers. Data that is excluded from the Act are protected health information and records.

The Act uses the terms "controller" and "processor." Under the Act, processors must assist controllers in meeting their obligations, including responding to consumer requests and conducting data protection assessments. If a controller sells sensitive data or biometric data, it must post a specific notice that it may use or sell your sensitive/biometric data in its privacy notice.

Consumers will have rights to: (1) confirm whether a controller is processing their personal data and access such personal data; (2) correct inaccuracies in the consumer 's personal data; (3) delete personal data provided by or obtained about the consumer; (4) obtain a portable copy of the consumer's personal data and (5) opt-out of processing for purposes of targeted advertising, the sale of personal data or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. The Act requires controllers to implement opt-out preference signals by January 1, 2025.

Controllers must obtain consent before processing a consumer's sensitive data. Sensitive data is defined as personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health diagnosis, sexuality, or citizenship or immigration status; genetic or biometric data processed to identify individuals; personal data collected from a known child; and precise geolocation data (*i.e.*, identifies a consumer within a radius of 1,750 ft.). Photographs of consumers are excluded from the Act.

The Texas Attorney General has the exclusive authority to enforce the Act. The Act provides controllers and processors with a 30-day cure period, which will not expire. The Office of the Attorney General (OAG) has exclusive authority to enforce the provisions of this new law and may obtain injunctive relief, civil penalties of up to $7,500 per violation, and reasonable attorneys' fees and investigative expenses. Penalties recovered are to be deposited in the general revenue fund.

If the OAG has "reasonable cause to believe" that a person has engaged in, is engaging in, or is about to engage in a violation of this bill, the OAG may issue a civil investigative demand (CID). The bill specifically authorizes the OAG to issue CIDs to controllers requesting relevant data protection assessments and requires controllers to provide those to the OAG. These assessments are confidential and exempt from the Texas Public Information Act, and disclosure to the OAG is not waiver of attorney client or work product privilege regarding information in the assessment. The procedure for CIDs is those established under Texas Business & Commerce Code, Section 15.10.

Federal Online Privacy Act

HR 2701 was introduced in the 118th United States Congress on January 24, 2023, by Congresswomen Anna Eshoo (D-CA) and Zoe Lofgren (D-CA). The 150-page bill would create a comprehensive framework for protecting consumer privacy online. It would give consumers more control over their data, require companies to be more transparent about their data practices, and establish new data security standards. The Online Privacy Act of 2023 (OPA) is a comprehensive piece of legislation that aims to safeguard the privacy of individuals in the digital age.

The OPA would regulate any entity including non-profits and common carriers that intentionally collects, processes, or maintains personal information and transmits personal information over an electronic network.

The OPA would establish an independent agency, the Digital Privacy Agency (DPA), to enforce the law and protect consumer privacy rights. The OPA seeks to establish a robust framework for data protection and empower consumers with greater control over their personal information, for longer than expressly consented to by the individual.

The director of the DPA would be appointed by the U.S. President and confirmed by the U.S. Senate for a six-year term. The DPS would have the power to issue regulations to implement the OPA and impose fines of up to $443.79 for each violation. The OPA would also empower State Attorneys General to enforce violations of the OPA and grant individuals a private right of action.

The OPA's key provisions and obligations include providing individuals with the right to access, correct, delete their personal information, as well as to opt out of the sale of their data. Entities that collect personal information must limit such collection to what is reasonably necessary for specified purposes. The data collecting entity must articulate the need for and minimize the

user data they collect, process, disclose, and maintain. The OPA requires entities to provide clear and conspicuous privacy notices that inform individuals about their data practices. Under this Act, entities must implement reasonable security measures to protect personal information from unauthorized access, use, or disclosure. Entities must minimize employee and contractor access to user data. They must not disclose or sell personal information without explicit consent.

The OPA has been praised by privacy advocates for its comprehensive approach to data protection. However, some industry groups have expressed concerns that the bill's requirements could be burdensome and stifle innovation. The bill's support is split along party affiliation, with Democrats supporting the bill and Republicans opposing the bill. A similar version of this bill failed in the 2021 congressional session.

As of November 2023, the OPA is in the early stages of the legislative process. It has been referred to the House Energy and Commerce Committee for consideration. The bill's future is uncertain, but it has the potential to significantly reshape the online privacy landscape in the United States.

About the Author

Kellye Hughes is a family justice prosecutor in the Ellis County & District Attorneys' office, specializing in protective orders, mental health law, and child welfare law. She holds a J.D. degree from Texas Wesleyan University School of Law. She is a member of the State Bar of Texas and is a council member of the State Bar of Texas Computer & Technology Section for 2023–26.

Digital Dialogue Dilemma: Wiretapping Statutes and the Internet

By Shilpa Coorg

Across the country, there has been a recent surge in Internet consumer privacy litigation, including claims brought under the federal Wiretap Act[1] and similar state-specific privacy laws, such as the California Invasion of Privacy Act (CIPA)[2]. Although these statutes were passed decades ago, plaintiffs have recently started applying these statutes to claims arising out of newer Internet technologies. This article identifies two common types of privacy claims brought by plaintiffs against website owners under such statutes and examines potential defenses.

The Wiretap Act provides for damages where a person "intentionally uses, endeavors to use, or procures any other person to intercept" any wire, oral, or electronic communications.[3] Similarly, a person is liable for damages under CIPA if they "intentionally tap" or "willfully and without the consent of all parties to the communication" read or learn of contents of private communications.[4] The availability of steep statutory damages—$100 per day of violation or $10,000 for claims brought under the Wiretap Act and $5,000 per violation under CIPA—has made such claims attractive to the plaintiffs' bar. Lawsuits against defendants frequently assert claims under both the Wiretap Act and CIPA.

Recently, both statutes have become the basis for two different types of claims against website owners. First, plaintiffs may attack "chat functionality," claiming that websites with a "chat box" violate the Wiretap Act and/or CIPA because the chat is "recorded" without the consumer's consent. Second, plaintiffs may bring claims based on the website's use of a tracking software or pixel (like the Meta pixel) that analyzes consumers' interactions with the website for purposes of targeted advertising. This second type of claim has been brought not only against the creator/developer of the tracking software (tracker), but against website owners utilizing such software as well.

Some California courts have rejected the first type of claim because the intended recipient cannot unlawfully "intercept" or "eavesdrop" on its own communications under the relevant statutes, and any third-party service provider involved in recording the chat also operates as

---

1 18 U.S.C. § 2510, *et seq*.
2 CIPA, Cal. Penal Code § 630, *et seq*.
3 Wiretap Act, § 2510
4 CIPA, § 631

an agent of the intended recipient.[5] But other courts have permitted the claims to move forward if the chat functionality is provided by a third-party provider who has negotiated for the "capability" to use and/or monetize the information captured in the chats for its own purposes.[6]

With respect to the second type of claim (use of tracking software), case law is sparser. The reason for this is two-fold. First, alternative dispute resolution venues, and not state or federal courts, have been particularly popular forums for these claims. Many companies have terms and conditions governing the use of their website that not only prohibit class action litigation but also require all disputes to be resolved through mandatory arbitration. Second, for cases that do get filed in federal or state courts, earlier settlements are typically the norm. Accordingly, the law around consumer internet privacy cases brought against third-party websites for their use of tracking pixels is relatively new and untested.

In theory, there are several defenses that can be asserted in these "tracking software" cases. As a threshold matter, defendants should determine whether state-specific statutes like CIPA even apply in the first instance. The website's terms and conditions may preclude application of state-specific laws based on the specified choice of law governing consumer disputes.

To the extent one or more privacy statutes can be applied, defendants may want to analyze whether the consent defense is available. The Wiretap Act is a "one-party" consent statute, and there could conceivably be consent so long as the website owner/operator is aware of the extent of transmission of data to the tracker and consents.[7]

Moreover, depending on the tracking pixel at issue, the website owner may never receive or have access to any user-specific data at any time. Rather, it is possible the tracking software

---

5 *See Martin v. Sephora USA, Inc.,* 2023 WL 2717636, at *7-10 (E.D. Cal. Mar. 30, 2023), report and recommendation adopted, 2023 WL 3061957 (E.D. Cal. Apr. 24, 2023); *Licea v. Am. Eagle Outfitters, Inc.,* 2023 WL 2469630, at *6-8 (C.D. Cal. Mar. 7, 2023); *Swarts v. Home Depot, Inc.,* 2023 WL 5615453 (N.D. Cal. Aug. 30, 2023)

6 *See Javier v. Assurance IQ, LLC,* 649 F.Supp.3d 891, 900-01 (N.D. Cal. 2023); *see also Wright v. Ulta Salon, Cosmetics, & Fragrance, Inc.*, 2023 WL 5837492, at *5-6 (S.D. Cal. Sept. 8, 2023)

7 18 U.S.C. § 2511(2)(d); *Doe v. Meta Platforms, Inc.*, 2023 WL 5837443, at *5 (N.D. Cal. Sept. 7, 2023) (denying motion to dismiss claims against tracker because determination of consent depended on the website owner's knowledge). Similarly, CIPA provides that parties to the communication cannot be held liable for "intercepting" communications to themselves. *In re: Nickelodeon Consumer Privacy Litigation,* 827 F.3d 262, 276 (3d Cir. 2016) (dismissing Wiretap Act and CIPA claims because neither apply "when the alleged interceptor was a party to the communications.").

automatically "pulls" information directly from the consumer's browser and matches that information to the consumer's account with the tracker, if the consumer has one. The website owner then typically receives an aggregated report (devoid of personally identifiable information) which can be used for marketing purposes. Critically, the consumer would likely have consented to the tracker's terms of use, which presumably should have disclosed all the ways in which the consumer's information might be collected and used (including from activity on third-party websites).[8]

***

Given the law regarding these topics is currently in flux, the safest approach may be for website owners and operators to add warnings and/or required opt-ins to their policies regarding chat recording, cookie usage, or other data sharing methods. While not bullet proof, proactively taking steps to minimize risk through clear disclosure and mandatory consumer consent may make companies a less convenient target for the plaintiffs' bar.

[8] *E.g., Smith v. Facebook, Inc., et al.,* 262 F.Supp.3d 943 (N.D. Cal. 2017) (granting motion to dismiss Wiretap Act claims because plaintiffs consented to Facebook's terms and conditions, which disclosed that Facebook collects information about users who visit third-party websites).

About the Author

Shilpa Coorg is Shilpa Coorg is an experienced litigator who handles all aspects of civil litigation. Her practice focuses on intellectual property litigation and counseling. Her patent expertise spans a broad range of technologies, including medical device, pharmaceutical generic product, smartphone, hardware, software, and telecommunication, as well as design patents. Shilpa is also well-versed in a wide variety of other areas of litigation, including contract, copyright, trademark, Lanham Act cases, Proposition 65 cases, and business disputes. She has routinely taken a leading role in bet-the-company cases from pre-filing through trial.

Prior to joining DTO, Shilpa developed her practice at Kirkland & Ellis LLP and Winston & Strawn LLP. During her time at Winston & Strawn, Shilpa argued and secured a denial of a motion for preliminary injunction brought against her client. On several occasions, she has successfully obtained dismissal on the papers for her Fortune 500 clients.

Shilpa is committed to supporting and mentoring other members of the Southern California legal community. She is the author of a well-received series of articles published in The Recorder on navigating legal practice as a Millennial attorney. As a former Co-President of SABA-SC (South Asian Bar Association of Southern California) and current member of the SABA-SC Steering Committee, Shilpa remains dedicated to the professional development of South Asian lawyers and law students, including through SABA-SC's Mentorship Program. She also leads the firm's Diversity, Equity, and Inclusion efforts as Chair of the firm's DEI Committee.

In her spare time, Shilpa enjoys baking, yoga, and travelling.

The Role of Technology in Accessible Dispute Resolution

By Denise Peterson

Traditionally, dispute resolutions were usually conducted via in-person proceedings , and online dispute resolution was more aspirational than actual. Before the spring of 2020, my mediation practice was overwhelmingly offline . I would routinely achieve more than the recommended 10,000 daily steps from looping the hallways between meeting rooms as I worked with different parties in person.

Now, I only break that 10,000 daily steps a handful of times a month. The rest of the time, I am online, usually on Zoom, engaging with attorneys and parties to resolve their cases in mediation or arbitration.

Over the past three years, with some trial and error, my tech setup has become pretty solid. Alienware laptop, ring lights, Yeti mics , and high-end cameras make me look and sound good. My carefully curated technology choices work well for me, but that is not always true for my clients, especially those with disabilities. It is not enough to ensure that I have what I need to meaningfully engage online; my responsibility is to ensure my parties can equally participate.

Before discussing the accessibility issues that arise from online dispute resolution, let's talk about the tremendous amount of good that has come from this seismic shift in how these legal services take place. One in four Americans has a disability, according to the Centers for Disease Control (CDC). These 89.6 million Americans may have mobility, cognition, independent living, hearing, vision, or self-care issues. They may also have disabilities from more than one category, complicating their challenges.

For those with mobility disabilities, online dispute resolution has enabled fuller participation without worrying about transportation, parking, and accommodations like fully accessible bathrooms. For the deaf community, scheduling sign language interpreters and translators became more accessible as the geographic location of the translator became less of a concern. Online communication software, such as Zoom, have integrated options that allow sign language interpreters to appear in a window next to their client for live closed captioning, and there are evolving AI technologies that enable live translations. Additionally, online communication programs such as Zoom and Teams are designed to work seamlessly without a mouse or other pointer device (entirely via a keyboard). And for many parties, being able to

appear from their home has lowered the stress and anxiety of litigation, enabling better engagement with the process.

Just because a technological solution exists does not mean that it will be appropriate or even practical. The rapid expansion of online dispute resolution has glossed over existing issues for those with disabilities and created new ones. The CDC defines disability as "any condition of the body or mind (impairment) that makes it more difficult for the person with the condition to do certain activities (activity limitation) and interact with the world around them (participation restrictions)." What is often assumed by the non-disabled is that one of these conditions will be visible or easily detected, and that is often not the case. Because of the stigma attached to disabilities, many with disabilities are uncomfortable expressing their need for accommodations, even to their own attorneys. The third leading cause of barriers to access for those with disabilities is the attitudes and stereotypes that surround being disabled.[1]

Assumptions are often made that those with disabilities already have what they need to function in an online space. However, the second most common barrier[2] to meaningful access for those with disabilities is the lack of relevant assistive, adaptive, and rehabilitation technology. And one of the most significant barriers to having those technologies is their cost. The poverty rate for adults with disabilities is twice that of non-disabled adults (27% compared to 12%),[3] which is more than twenty-four million adults.

People with sight loss may be unable to afford screen readers, those with dyslexia or cognitive issues may need text-to-speech software, and reduced-cost versions of that software are often restricted to educational uses only. And that is with the assumption that the person needing them can afford a smartphone or computer that is powerful enough to run those kind of software.

So, how do we, as attorneys and dispute resolution professionals, ensure that our clients have the appropriate technology so that they are meaningfully able to engage in online dispute resolution?

---

1 See: https://www.cdc.gov/ncbddd/disabilityandhealth/disability-barriers.html

2 id

3 See: National Disability Institute, Financial Inequality: Disability, Race, and Poverty in America: https://www.nationaldisabilityinstitute.org/wp-content/uploads/2019/02/disability-race-poverty-in-america.pdf

First, make no assumptions about whether or not someone has a disability. Screen all of your clients equally. This can be done during your standard intake procedures. The following questions are some ways to begin screening. The following is a non-exhaustive list, and depending on your client's answer, more questions may need to be asked.

- If this case is mediated online, will you use a phone or a laptop?
- Will you be using any assistive technology such as a screen reader?
- Do you have a private, quiet space from which you can use to mediate?
- Will you need the assistance of a translator?
- Do you have any difficulty hearing?
- Mediation online often means sitting or staying in the same place for four or more hours. Are you comfortable with this?

Screening can also identify when online mediation may not be the best option. Someone with a shared living situation and difficulty hearing may not be a good candidate for an online mediation. They may do better in person, whether in the attorney's office or at a mediation center.

Good questions can also identify when we have to move away from the "standard approaches" for mediation lengths. Someone with a chronic illness may have a problem that requires a full day of mediation, but their condition will make it hard for them to be focused for that long. The parties and the mediator may have to work out a plan for several days worth of sessions.

Technology has brought meaningful changes to the practice of dispute resolution. However, those changes also demand holistically evaluating its appropriate use on a case-by-case basis for each client. The conveniences of tedchnolgy must not come at the expense of our clients' meaningful engagement.

About the Author

Denise Peterson is a full-time mediator and arbitrator at her firm PetersonADR. In the fall of 2022, she joined South Texas College of Law Houston as an adjunct professor and "pracademic" in dispute resolution. She teaches both the mediation clinic and negotiation classes. She graduated from South Texas College of Law Houston in 2010 and became an associate for Morgan Lewis, working on matters relating to the housing crisis, asbestos defense, employment, and general civil litigation. She is licensed in Texas and New York and is a qualified solicitor to the senior courts of England and Wales. She is a Fellow of the Chartered Institute of Arbitrators and co-chair of the Texas section of the North American Branch. Currently pursuing her master's in legal history, she writes and speaks frequently on dispute resolution, arbitration, mediation, negotiation, implicit bias, and Houston's civil rights history.

The Nature of Consent Matters in DNA Analysis Cases

By Pierre Grosdidier

Arizona authorities learned that consenting to a DNA analysis in a criminal case for a specific purpose does not give authorities the right to exploit the DNA in another criminal case without a warrant.[1]

In January 2015, Ian Mitcham consented to have his blood drawn for alcohol and drug tests after his arrest for driving under the influence. His consent form said nothing about other tests, and he consented only for the purpose of these tests. Moreover, an unused back-up blood sample was to be destroyed after 90 days. It was not. A month later, in February 2015, authorities investigated a woman's brutal sexual assault and murder. They developed a DNA profile based on crime scene evidence but could not match it to a suspect in the CODIS database.[2]

The case remained unsolved until 2018 when familial DNA analyses based on the crime scene sample led authorities to Mitcham via his incarcerated brother. Without securing a warrant, authorities then analyzed Mitcham's remaining blood sample and successfully matched it to the murder suspect. Mitcham was arrested and charged, and his DNA re-sampled with a buccal swab in accordance with standard booking procedures. Mitcham moved to suppress the DNA evidence from his 2015 arrest on the ground that the 2018 test "went far beyond the scope" of his 2015 consent, and also that of the booking buccal sample because it was the fruit of the poisonous tree. The trial court agreed and granted the motion. The Court of appeal agreed that the 2018 test on the 2015 sample was improper, but reversed because authorities would have identified and arrested Mitcham even without it.[3]

---

1 *State v. Mitcham*, 535 P.3d 948 (Ariz. App. 2023); *see also Doe v. City and County of San Francisco*, No. 3:22-cv-05179-AGT, ECF # 40 (N.D. Cal. July 20, 2023) (holding that Doe alleged a plausible Fourth Amendment claim when police used her DNA to investigate criminal cases in which she was allegedly involved, when she had only agreed to provide her DNA to investigate her sexual assault complaint).

2 For a simple explanation of how CODIS works, *see* Pierre Grosdidier, *A lawyer's genetic fingerprinting primer*, Circuits, June 2019, p. 81 (available at https://sbot.org/circuits/page/2/).

3 *Mitcham*, 535 P.3d at 950-51.

The Court first distinguished between a judicial order to take a buccal cell sample and the latter's DNA analysis for CODIS markers. It held that the first was indistinguishable from the taking of a fingerprint but that the latter required probable cause or reasonable suspicion, but not necessarily a warrant because of the limited information CODIS makers provide. The Court described these markers, not known to contain any personal medical information,[4] as no more intrusive than a suitcase's nametag or a car's license plate. Moreover, CODIS markers are not, in and of themselves, evidence of a crime unlike the result of a blood test for alcohol or drugs.[5]

Turning to the case at hand, the Court held that the police's 2018 DNA analysis of the 2015 sample exceeded Mitcham's consent and amounted to an unlawful Fourth Amendment search. It rejected the State's argument that possession of the back-up blood sample meant that the Fourth Amendment was no longer implicated. Possession of property does not give authorities *carte blanche* to dispose of it untethered. Possession of a properly seized trunk or telephone does not automatically authorize the search of their contents because their owners still retain a privacy interest in these contents. A blood sample containing DNA information is no different.[6]

Despite concurring with the trial court that the 2018 DNA analysis of the 2015 sample was unlawful, the Court rejected the trial court's application of the exclusionary rule and reversed the suppression order. It held that the police had enough evidence and, therefore probable cause, to arrest Mitcham even without the 2015 sample's DNA. The crime scene DNA matched that of a first-degree relative of Mitcham's incarcerated brother, either his father, son, or brother. The inmate's father had passed away, his two sons lived out of state, and his two brothers lived in Phoenix, one of whom was Ian Mitcham. Moreover, the latter lived close to the victim. These facts alone established probable cause for an arrest, which "is present when the arresting officer knows 'facts and circumstances ... sufficient to warrant a man of reasonable caution to believe that a felony had been committed by the person arrested.'" Once Mitcham had been arrested, a DNA test would have confirmed that his DNA matched that of the crime scene.[7]

---

4 *See* Jayann Sepich, *Arrestee DNA solves crimes and saves lives*, Circuits, June 2019, p. 55.

5 *Mitcham*, 535 P.3d at 652–55.

6 *Id*. at 955–57.

7 *Id*. at 956–59.

About the Author

Pierre Grosdidier is a litigation attorney in Houston. He is board certified in construction law by the Texas Board of Legal Specialization. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Chair for 2022–23. He was elected Medium Section Representative to the State Bar of Texas for the 2023–26 term.

Fourth Amendment Does Not Prohibit Using iPhone Camera to See Through Tinted Car Windows

By Pierre Grosdidier

Defendant Christopher Poller learned the hard way that the Fourth Amendment's prohibition against unreasonable searches did not protect him when authorities used an iPhone to see through his car's heavily tinted windows.[1] A detective looked inside Poller's publicly parked car with an iPhone held up against its otherwise opaque windows and, using the device's viewfinder app, spotted guns inside. The detective then cupped his hands around his eyes to peer inside the car (without touching the windshield) and saw what looked like a bag of heroin on the passenger seat. These observations supported a search warrant that led to federal charges based on the seized contraband. The district court denied Poller's motion to suppress the evidence on Fourth Amendment grounds.[2] Poller argued both that the police invaded his reasonable subjective expectation of privacy and that the use of the iPhone against his car's windows was a physical trespass on his property.

Both sides agreed that peering inside a stopped vehicle without touching it to see if it contains contraband, even with the help of a flashlight, does not offend the Fourth Amendment.[3] Instead, Poller analogized his situation to that in *Kyllo v. United States*, where the United States Supreme Court held that authorities violated the Fourth Amendment when they used thermal imaging cameras to survey a home and detect the heat signature of lamps used to grow marijuana.[4] But, *Kyllo* turned on the fact that authorities used "a device that [wa]s not in general public use," *i.e.*, the thermal imaging devices, to probe "details of the home" that would have been otherwise inscrutable without a physical entry.[5]

Here, Poller did not argue that iPhone and their cameras are not in general public use. Nor could he do so given the ubiquitousness of these devices, which the U.S. Supreme Court has casually compared to "an important feature of human anatomy."[6] It did not help Poller that Internet is rife with stories that report that thieves can see through tinted car windows with cell

---

1 *United States v. Poller*, No. 3:22-cr-165 (JAM), 2023 WL 4535338, at *1 (D. Conn. July 14, 2023).

2 *Id.* at **1-2. Poller subsequently entered into a conditional plea agreement reserving the right to appeal the Court's order. Pacer ECF 51.

3 *Poller*, 2023 WL 4535338, at *2 (citing *Texas v. Brown*, 460 U.S. 730, 739-40 (1983)).

4 *Id.* (citing *Kyllo v. United States*, 533 U.S. 27 (2001)).

5 *Id.* at *3 (citing *Kyllo*, 533 U.S. at 40).

6 *Id.* (citing *Riley v. California*, 573 U.S. 373, 385 (2014)).

phone cameras, which confirmed their general use for snooping.[7] Thus, the detective's iPhone use to peer inside Poller's car did not infringe the latter's subjective expectation of privacy.

The Court also rejected Poller's physical intrusion argument. It is well established that the Fourth Amendment does not protect things that are exposed to public view. Thus, police officers need not avert looking into protected spaces visible from the thoroughfare. But it does not take much to physically intrude into a protected space, as when officers insert a key into a car lock to check its ownership, or when they step onto a driveway to touch a car's hood to check its temperature.[8]

Poller alleged that the detective intruded into his private sphere when his iPhone touched the car's tinted windows to see inside. But such contact was not necessary for the initial search. Body-cam videos of the incident showed that the iPhone still revealed what was inside the car even after the detective lifted the device away from the window. Moreover, the detective could also see inside the car with his cupped hands around his eyes without touching the windshield. Other courts have denied motions to suppress when police engaged in "minor physical contact with a car" that was "incidental and not necessary" to acquire the challenged evidence.[9] The Court concluded that even though the police conducted a Fourth Amendment search to the extent they made physical contact with the car to determine what it contained, the Court denied Poller's motion to suppress because the record did not show that such contact was necessary to achieve this end.

---

7 *Id.*

8 *Id.* at *4 (citing cases).

9 *Id.* (citing cases).

About the Author

Pierre Grosdidier is a litigation attorney in Houston. He is board certified in construction law by the Texas Board of Legal Specialization. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Chair for 2022–23. He was elected Medium Section Representative to the State Bar of Texas for the 2023–26 term.

Fourth Amendment Rights Do Not Extend to Another Person's Privacy Violation

By Pierre Grosdidier

The Fourth Amendment protects "the right of the people to be secure in *their* persons, houses, papers, and effects[.]"[1] Two cases out of the Fifth Circuit Court of Appeals illustrate the Fourth Amendment's standing principle, which states that an unreasonable search must infringe a person's own rights, not those of another person in a criminal matter.

Louisiana authorities expected Matthew Beaudion and Jessica Davis to run meth from Houston to Monroe.[2] They obtained a search warrant for the GPS coordinates of Davis's cell phone for a sixteen-hour time window. Six specific coordinate requests to Davis's cellular phone company allowed them to track and arrest the pair, search their car, and find the meth. Beaudion pleaded guilty to drug charges after the court denied his motion to suppress on the basis that the GPS tracking warrant was defective. He appealed, but the Fifth Circuit affirmed.[3]

As the Court demonstrated in a concise and enlightening history of the Fourth Amendment's origins under English and Colonial law, a person must show the injury of a personalized interest to assert a Fourth Amendment claim.[4] This injury can take the form of a physical intrusion in a protected space in which the person has a property interest, or a violation of the person's subjective reasonable expectation of privacy. Here, the "place searched" was Davis's phone's GPS coordinates. The Court rejected Beaudion's argument that the search extended to his person because he was its target. A search is defined by its scope, not its target, and the warrant's scope extended only to the GPS coordinates.[5]

Moreover, Beaudion had no legitimate expectation of privacy in Davis's phone. It did not matter that he originally purchased the phone because he lost his interest in it when he gifted it to Davis, and his personal use of the phone in Davis's presence was not sufficiently in evidence in the record to matter. Davis retained possession of the phone, was its primary user, and had her

---

1 U.S. Const. amend. VI (emphasis added).

2 *United States v. Beaudion*, 979 F.3d 1092, 1093–94 (5th Cir. 2020).

3 Beaudion did not challenge the constitutionality of his traffic stop in the trial court, erroneously so, it appears. *Id.* at 1101–02.

4 *Id.* at 1094–96.

5 *Id.* at 1097–99.

parents pay for its service. Even if Beaudion has an expectation of privacy, the Court could not find that it was reasonable.[6]

The same result issued in *United States v. Gaulden*, a more recent case.[7] Kentrell Gaulden, a rapper and a felon, was arrested on weapons charges. At trial, prosecutors offered incriminating videos recovered from a memory card showing Gaulden illegally manipulating firearms. Gaulden successfully suppressed the videos, but the Fifth Circuit reversed, holding that Gaulden had no protected interest in them.[8]

A third-party cameraman hired by Gaulden's own company recorded the videos, which Gaulden used for promotional purposes on social media. But Gaulden never established a property interest in the videos, and the Court rejected his argument that he retained such an interest because he exerted the right to select which videos to display. The cameraman owned both his camera and the memory card, and the company paid for his services. Under Louisiana law, ownership in an entity does not convey ownership in the entity's property and, in any event, payment for videographic services does not automatically convey ownership in the work product.[9]

Additionally, it is well established under Fourth Amendment law that individuals have no legitimate expectation of privacy in information that they voluntarily surrender to third parties. Here, there was no evidence that Gaulden intended to keep the recordings private. To the contrary, the videographer was tasked with following him around, as in reality TV, for promotional reasons. Gaulden took the risk and could not complain that the videographer might release the videos, including those depicting him in public wielding weapons with his confederates.[10]

---

6 *Id.* at 1099.
7 73 F.4th 390, 391 (5th Cir. 2023).
8 *Id.* at 391–92.
9 *Id.* at 393.
10 *Id.* at 394–95.

About the Author

Pierre Grosdidier is a litigation attorney in Houston. He is board certified in construction law by the Texas Board of Legal Specialization. Pierre's practice also includes data privacy and unauthorized computer access issues and litigation. Prior to practicing law, Pierre worked in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas, an AAA Panelist, a registered P.E. in Texas (inactive), a member of the Texas Bar Foundation, a Fellow of the American Bar Foundation, and the State Bar of Texas Computer & Technology Section Chair for 2022–23. He was elected Medium Section Representative to the State Bar of Texas for the 2023–26 term.

Navigating the Legal Landscape for Kid Influencers

By Nick Polk

In a digital age where social media influencers hold significant sway over online audiences, a new legal frontier has emerged concerning kid influencers. Recent developments have shed light on the need for a comprehensive understanding of the legal considerations surrounding young individuals who wield influence on various platforms. Hopefully, this article will help navigate this complex landscape and ensure ethical and legal compliance.

The Rise of Kid Influencers

The meteoric rise of social media has given birth to a new generation of influencers, some of whom are barely old enough to have a social media account. These "kid influencers" have gained popularity for their relatable content and genuine interactions with their audience. However, this newfound fame also raises questions about the legalities surrounding their online presence.

Legal Considerations

The legal implications of having children as social media influencers extend beyond mere content creation. There are several key aspects that need to be carefully addressed:

1. Child Labor Laws: Kid influencers are often engaged in what can be considered as a form of work, even if i it is in the digital realm. **The Fair Labor Standards Act (FLSA)** in the United States sets standards for child labor, including working hours, types of work allowed, and age restrictions. It is essential to adhere to these laws to ensure that their participation in content creation remains within legal boundaries.

The FLSA explains:

> "Oppressive child labor" means a condition of employment under which...any employee under the age of sixteen years is employed by an employer (other than a parent or a person standing in place of a parent employing his own child or a child in his custody) under the age of sixteen years in an occupation other than manufacturing or mining or an occupation found by the Secretary of Labor to be particularly hazardous for the

> employment of children between the ages of sixteen and eighteen years or detrimental to their health or well-being.[1]

This could mean that if a child social media influencer is required to work long hours, engage in dangerous or unhealthy activities, or produce content that is sexually suggestive or otherwise inappropriate, their working conditions could be considered to be oppressive. Additionally, if a child social media influencer is prevented from attending school or engaging in other essential activities due to their work, their working conditions could also be considered to be oppressive.

In the Illinois' Public Act 103-0556, there are even new, specific regulations addressing child social media influencers. **It is important for Illinois adult guardians of these young social media influencers to keep the following records:**[2]

1. Name and documentary proof of age of the minor engaged in the work of vlogging.
2. Number of vlogs that generated compensation during the reporting period
3. Total number of minutes of the vlogs that the vlogger received compensation for during the reporting period.
4. Total number of minutes each minor was featured in vlogs during the reporting period.
5. Total compensation generated from vlogs featuring a minor during the reporting period.
6. Amount deposited into the trust account for the benefit of the minor engaged in the working of vlogging.

2. Privacy and Consent: Kid influencers are protected by privacy laws just like any other individual. **The Children's Online Privacy Protection Act (COPPA)** in the U.S. requires obtaining verifiable parental consent before collecting personal information from children under 13.

COPPA explains the general requirements for parental consent:[3]

> (1) An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

---

1 29 USC § 203(l)

2 Illinois General Assembly, 2023, Public Act 103-0556, Sec. 2.6(c)

3 https://www.ecfr.gov/current/title-16/section-312.5

(2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

Additionally, the General Data Protection Regulation (GDPR) in the European Union has specific provisions for processing personal data of children. Obtaining proper consent from parents or guardians is crucial before sharing any personal information or images of these young individuals.

3. Advertising and Endorsements: As kid influencers often collaborate with brands, there's a need to disclose any paid partnerships transparently. **The Federal Trade Commission (FTC)** mandates clear and conspicuous disclosure of such relationships. The FTC's Endorsement Guides provide guidelines on how to properly disclose material connections between influencers and brands, ensuring transparency and credibility in online advertising.

Here are some general endorsement guidelines you and your child should follow:[4]

(a) Endorsements must reflect the honest opinions, findings, beliefs, or experience of the endorser. Furthermore, an endorsement may not convey any express or implied representation that would be deceptive if made directly by the advertiser.

(b) The endorsement message need not be phrased in the exact words of the endorser, unless the advertisement affirmatively so represents. However, the endorsement may not be presented out of context or reworded so as to distort in any way the endorser's opinion or experience with the product.

(c) When the advertisement represents that the endorser uses the endorsed product, the endorser must have been a bona fide user of it at the time the endorsement was given. Additionally, the advertiser may continue to run the advertisement only so long as it has good reason to believe that the endorser remains a bona fide user of the product.

As a parent, you should encourage your child to be honest and authentic in their endorsements. They should only endorse products or services that they truly believe in. Be an active partner in evaluating the products or services they are endorsing and make their own decisions about whether or not to recommend them to their followers. Make sure your child is aware of the risks associated with social media and how to protect themselves. Having an

---

[4] https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-publishes-final-guides-governing-endorsements-testimonials/091005revisedendorsementguides.pdf

attorney can help you answer questions and make sure you are following all necessary guidelines and procedures.

4. Intellectual Property: Whether it is the content they create or their likeness, intellectual property rights must be respected. Kid influencers and their legal guardians need to understand how their creations can be used and protected. Copyright law safeguards original creative works, and trademarks protect branding elements. It is essential to ensure that content shared on social media does not infringe upon the intellectual property rights of others.

The world of kid influencers brings both excitement and responsibility. As these young individuals share their voices and stories with the world, it is our collective duty to ensure their online presence is managed with care, ethics, and compliance, enabling kid influencers to thrive while respecting the law.

About the Author

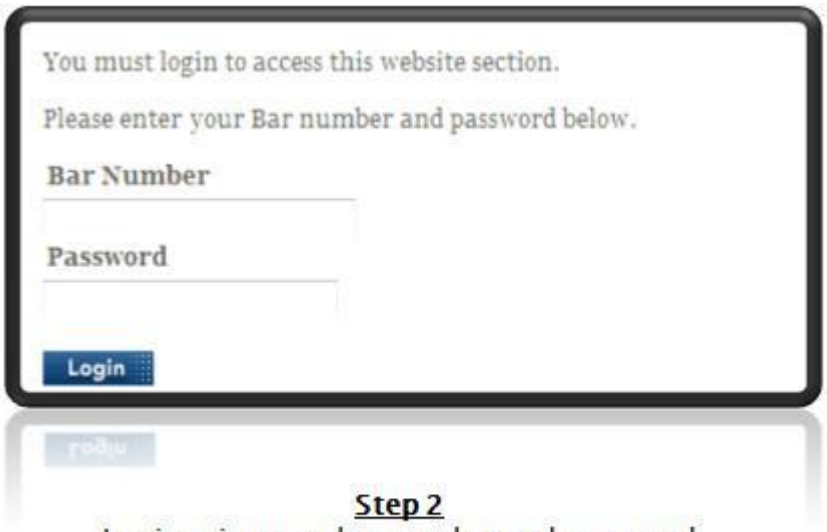
Nick Polk is an accomplished professional who has recently assumed the role of Social Media Director at Mudd Law. With a strong background in fundraising and administrative coordination, Nick brings his expertise to further the mission and goals of the organization through strategic social media initiatives. Previously, he played a pivotal role as the Development and Administrative Coordinator at the Foundation for Sarcoidosis Research (FSR), where he effectively supported fundraising efforts and established meaningful connections with donors.

Nick's journey began with a degree in Comedy Writing and Performance from Columbia College Chicago. Since then, he has lent his talents to various non-profit organizations, including Northwestern Memorial Foundation and Rotary International. His enthusiasm for fundraising campaigns has been evident throughout his career, and now, as the Social Media Coordinator at Mudd Law, he is excited to leverage his skills to contribute to the Mudd Law team.

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:

Reginald Hirsch – Houston – Chair

William Smith – Austin – Chair-Elect

Lavonne Burke – Houston – Treasurer

Mitch Zoll – Austin – Secretary

Pierre Grosdidier – Houston

– Immediate Past Chair

Circuits Editors:

Sally Pretorius – Dallas

Katie Stahl – Houston

Committee Chairs:

Sally Pretorius – Dallas

– Circuits eJournal Co-Chair

Katie Stahl – Houston

– Circuits eJournal Co-Chair

Grecia Martinez – Dallas

– CLE Program Coordinator

Mark Unger – San Antonio

– App committee Co-Chair

Mitch Zoll – Austin

– Tech Competency Chair

Mitch Zoll – Austin

– Speaker's Bureau

Webmaster:

Ron Chichester – Houston

Appointed Judicial Members:

Judge Xavier Rodriguez – San Antonio

Hon. Roy Ferguson – Alpine

Hon. Emily Miskel – McKinney

Term Expiring 2024:

Justin Freeman – Austin

Zachary Herbert – Dallas

Grecia Martinez – Dallas

Guillermo "Will" Trevino – Brownsville

Term Expiring 2025:

Alan Cooper – Dallas

Mason Fitch – Houston

A. Dawson Lightfoot – Dallas

Sally Pretorius – Dallas

Term Expiring 2026:

Sean Hamada – Dallas

Kellye Hughes – Waxahachie

Sanjeev Kumar – Austin

Katie Stahl – Houston

Chairs of the Computer & Technology Section

2023–2024: Reginald A. Hirsch
2022–2023: Pierre Grosdidier
2021–2022: Elizabeth Rogers
2020–2021: Shawn Tuma
2019–2020: John Browning
2018–2019: Sammy Ford IV
2017–2018: Michael Curran
2016–2017: Shannon Warren
2015–2016: Craig Ball
2014–2015: Joseph Jacobson
2013–2014: Antony P. Ng
2012–2013: Thomas Jason Smith
2011–2012: Ralph H. Brock
2010–2011: Grant Matthew Scheiner
2009–2010: Josiah Q. Hamilton
2008–2009: Ronald Lyle Chichester
2007–2008: Mark Ilan Unger
2006–2007: Michael David Peck
2005–2006: Robert A. Ray
2004–2005: James E. Hambleton
2003–2004: Jason Scott Coomer
2002–2003: Curt B. Henderson
2001–2002: Clint Foster Sare
2000–2001: Lisa Lynn Meyerhoff
1999–2000: Patrick D. Mahoney
1998–1999: Tamara L. Kurtz
1997–1998: William L. Lafuze
1996–1997: William Bates Roberts
1995–1996: Al Harrison
1994–1995: Herbert J. Hammond
1993–1994: Robert D. Kimball
1992–1993: Raymond T. Nimmer
1991–1992: Peter S. Vogel
1990–1991: Peter S. Vogel