COMPUTER AND TECHNOLOGY SECTION

CIRCUITS

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

March 2025

SECTION LEADERSHIP

William Smith, *Chair*
Lavonne Burke Hopkins, *Chair-Elect*
Mitch Zoll, *Treasurer*
Grecia Martinez, *Secretary*
Katie Stahl, *e-Journal Co-Editor*
Aaron Woo, *e-Journal Co-Editor*
Sally Pretorius, *CLE Committee Chair*
Reginald Hirsch, *Imm. Past Chair*

COUNCIL MEMBERS

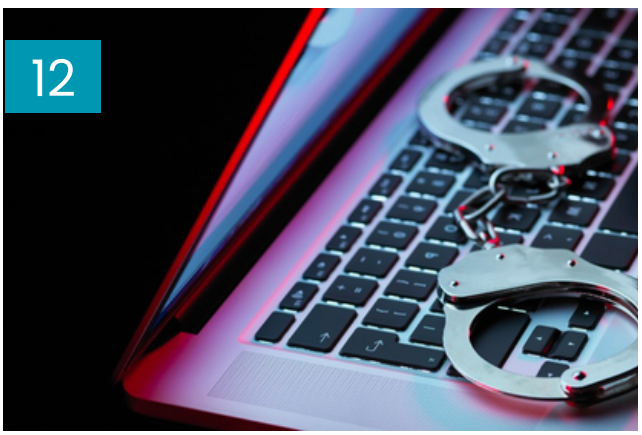
Maria Moffett
A. Dawson Lightfoot
Sally Pretorius
Sean Hamada
Kellye Hughes
Sanjeev Kumar
Katie Stahl
Lori Bellows
Tyler Bridegan
Liz Cantu
Aaron Woo

JUDICIAL APPOINTMENTS

Hon. Xavier Rodriguez
Hon. Roy Ferguson
Hon. Karin Crump

In This Issue:

Table of **CONTENTS**



Welcome to the March 2025 issue of Circuits! We're kicking off the year with a mix of cutting-edge topics, practical insights, and thought-provoking discussions that section members should have on their radar.

Technology is advancing at breakneck speed, and the legal landscape is shifting just as quickly.

This issue covers some of the most pressing topics, including:

- What Humans Can Learn from Conducting Discovery with Generative AI
- The Intersection of Psychology and Cybersecurity: Understanding Human Factors in Social Engineering
- Expansion and Retraction: Recent Developments in the Scope of Civil CFAA Litigation
- The Tariff Man: What to Expect from Trump's Second Term
- Optimizing Sales and Onboarding: Maximizing Technology to Streamline Your Workflow
- Authorities Cannot View Hash-Trapped Files Without a Warrant
- Transfers of Sensitive Personal Data to China, Cuba, Iran, North Korea, Russia, and Venezuela
- NIST Framework Small Business Quick Start Guide Applied for Solos
- Case Snippets

We're particularly excited about the diverse perspectives and expertise featured in this issue. Whether you're looking for strategic insights, legal analysis, or practical tech tips, there's something here for you.

We'd love to hear from you! If you have an idea for an article or a topic you'd like to see covered, reach out and let's keep the conversation going.
Enjoy the issue!

Please flip to the last page of the issue for information on the upcoming free online CLE: NAVIGATING THE FUTURE OF AI: LATEST DEVELOPMENTS IN AI REGULATION. We are excited to partner with the International Law Section to bring this CLE on March 21, 2025, from noon to 1 PM Central.

Katherine Stahl and Aaron Woo

Co-Editors, Circuits

Computer & Technology Section

State Bar of Texas

What Humans Can Learn from Conducting Discovery with Generative AI

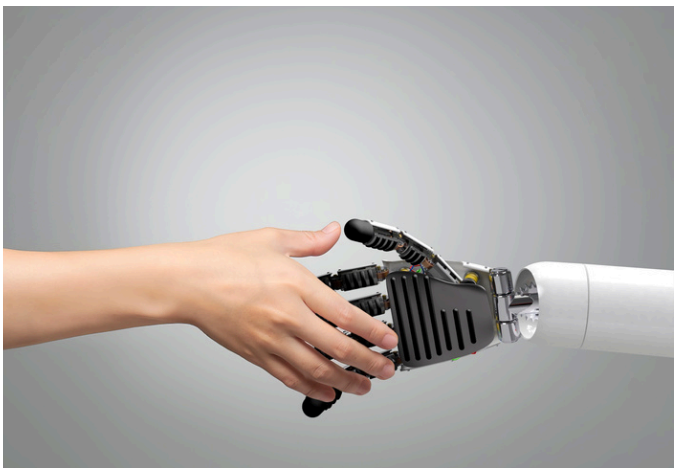
Introduction

We are past the early days of law firms using generative AI (GenAI) to conduct first-level document review. Instead, today it is common for law firms to use GenAI for increasingly complex searching and coding tasks that are critical to identifying and categorizing the most critical documents in a case, both for the purpose of producing those documents and for reviewing what is produced by opposing parties and third parties. And it is happening fast—both in terms of adoption and in terms of the speed with which reviews are being completed.

Having completed more than 80 independent GenAI document reviews on Syllo—including a number of GenAI to human review comparison studies— we are uniquely able to draw conclusions about the performance of GenAI in these reviews and share best practices for obtaining optimal results. In short, done correctly, GenAI review performs first-level document review with unprecedented speed and with coding that is consistently more accurate and more helpful to trial teams and second-level reviewers. More than any prior technology, GenAI facility allows case teams to rapidly analyze large volumes of electronically stored information (ESI), satisfy their discovery obligations, and get to the work of case building as quickly and efficiently as possible (in days, weeks, or months faster than your non-GenAI enabled counterparts).

How GenAI Document Reviews Work on Syllo

On Syllo, the process of setting up a GenAI Document review is very similar to the process firms undertake when working with a contracted human team. The attorneys litigating the case, or their paralegals or litigation support professionals, identify the universe of documents to be reviewed, which can be a set of documents collected from the client or a set of documents produced by an opposing party or a third party.



The attorneys then define the issues they will use to code the documents, just as they would with a human team. In a case in which documents collected from the client are to be coded, the tags applied may correspond directly to the Requests for Production served by the opposing party, for example. Where an opposing party's production or a third party's production is to be reviewed, coding may correspond to the reviewing party's Requests for Production or key issues in the case or both. Additional issue codes (as many as the case team needs) may also be defined to search for the most important (or "hot") documents.

The instructions for each issue code are input in a natural language format that often resembles the instructions, or issues, that would be provided to contract reviewers. In addition to these instructions, case teams provide information regarding the general facts of the litigation. For example, the case team identifies parties, witnesses, business entities, products, and properties central to the case, as well as potential privilege, date limitations, or other restrictive issues. Again, the information and the form in which it is provided is similar to how attorneys typically provide background information to a team of

contract reviewers.

Syllo's GenAI document review platform uses this information to apply tags to the documents reflecting these issue codes. Syllo then provides a hyperlinked table sorted by issue code that the case team can use to assess the number of documents tagged as relevant to each of these categories. Documents are also sorted by their degree of relevance to the tagged issue, meaning high priority documents will be the first ones recommended for further review. By clicking on the hyperlinks in the table, attorneys can conduct their secondary review of the tagged documents and building their case.

For each tag applied by the AI, the AI also provides a concise explanation as to why the document was tagged as relevant to a particular issue or discovery request.The case team or second-level reviewer can review the documents alongside the explanations provided by the system, and by clicking on an explanation, the attorney is directed to the relevant page of the document and the specific section of that page, with the key information highlighted.

Lessons Learned

A. GenAI Can Produce More Granularly Categorized Document Sets that Make Second-Level Review Far Less Taxing and Far More Efficient

Even the most advanced and experienced document review attorneys can generally keep at most 8 to 10 issues in mind as they code a document or universe of documents. GenAI, on the other hand, is capable of reviewing documents for far more issues than humans can. The ability to divide the documents into more specific categories has a significant impact on second-level review, and the ability to use second level review for strategic case building, rather than mere diligence. More specific categories translate to fewer documents to be reviewed in each category, simplifying the process of finding information relevant to an issue. Second-level review conducted by the case team is further aided by sorting the documents according to their degree of relevance. The second-level reviewer can immediately turn to the documents identified as most relevant rather than sorting through a larger set of documents that may have only tangential relevance to the issue.

In addition to the categorization of documents, GenAI provides a much more thorough work up of each document. Using traditional review techniques, the attorney conducting the second-level review is often presented simply with a document that has been tagged as relevant to a particular issue, or with a particular relevance score (with older technology-assisted-review technologies), without any further explanation as to why. Using GenAI, the second-level reviewer is provided with an explanation as to why the document was tagged and highlighting showing the relevant text. The highlighting and ability to navigate to the relevant section is particularly useful when reviewing large documents of 100 pages or more. These features enable the second-level reviewer to understand the relevance of the documents she is reviewing more quickly than under traditional methods.

B. GenAI Document Review Identifies a Higher Percentage of Relevant Documents Than Traditional Methods

In cases in which an attorney is producing documents in response to an opposing party's discovery requests, it is critical that any review process identify a high percentage of the relevant documents—everything that could possibly be responsive, with as little noise as possible.Syllo is nudged to be overinclusive by design and is highly effective in returning responsive documents.

Even so, case teams using GenAI document review should still conduct quality control to ensure that relevant documents are not omitted. This quality control review is typically done by the case team reviewing a statistically significant sample of documents that were not marked as relevant to any issues, i.e., the set of untagged documents. By conducting this analysis, case teams can estimate the percentage of relevant documents that were not identified and, correspondingly, the percentage of relevant documents identified. This latter percentage is known as the estimated recall rate. Such statistical validation methods have been endorsed by courts over the last ten-plus years of technology assisted review in litigation, and the same or similar validation methods can be, and routinely are,

applied to GenAI reviews.

Quality control testing on documents marked as responsive by Syllo have demonstrated GenAI's ability to identify a high percentage of relevant documents after the initial run of tagging. Case teams conducting this quality control review have validated estimated recall rates of 95% or more after the initial run. This compares very favorably to human review, which often tops out at around 80% of relevant documents identified after the initial review, and traditional technology-assisted review, which typically obtains about an 85% recall rate after the first review. In short, this approach to first-level document review is not merely about saving costs and streamlining litigation (though those are major benefits), but it also can be defended as a superior approach as to quality as well.

C. GenAI Document Review Will Impact the Speed of Litigation and Litigation Tactics

GenAI document reviews are fast, with hundreds of thousands or even millions of documents reviewed in a week or two, compared to many months for typical human review teams. We anticipate that early adopters using this technology will use the speed with which they can review documents strategically, for example, by quickly identifying deficiencies in opposing parties' productions and pushing for missing documents, or noticing depositions weeks or months earlier than would normally be possible. Parties deploying this technology will also push for faster scheduling orders to put pressure on their opponents. Finally, because GenAI costs less than traditional review methods, parties that were traditionally willing to settle to avoid the expense of conducting document review may be less inclined to do so.

D. The Changing Role of Humans in Document Review

Even with the introduction of GenAI into the document review process, lawyers will continue to play a critical role in reviewing and producing documents. As described above, lawyers will assume responsibility for defining the issue tags, crafting the instructions used to apply those tags, and conducting the quality control process.

Through the quality control process, human reviewers ensure that GenAI isn't making fundamental errors in the analysis of documents. These errors could result in relevant documents being excluded from production or productions including a high percentage of non-responsive documents. Lawyers will sometimes need to refine their instructions based on their quality control or new things learned during the document review process, similar to how lawyers provide such instructions in traditional reviews. Fortunately, because GenAI is more uniform in its approach to tagging documents, these refinements are more likely to significantly improve results in a predictable way.

Conducting quality control analyses has an important secondary impact: it acquaints attorneys with their ultimate responsibility in checking GenAI outputs. Initial blunders with GenAI have occurred where attorneys have blindly trusted model outputs and submitted work product without checking it. By contrast, attorneys implementing these quality control processes will learn that responsibility remains with attorneys to ensure that the output of GenAI models is correct.

Conclusion

The growing adoption of GenAI to automate first-level document review is already changing the ways that attorneys approach discovery. GenAI offers the promise of reviews that identify more relevant documents, faster, and less expensively than human reviews. This means more time spent by attorneys on the higher-value aspects of litigation, less time spent by attorneys and courts mired in months and sometimes years of document discovery, and overall a lower cost of litigation for their clients.

These techniques are already allowing litigation teams who use them to more effectively understand facts and gain a strategic edge in litigation. However, attorneys retain ultimate responsibility for the accuracy of the output for this new approach to conducting discovery.

ABOUT THE AUTHORS

Jeff Chivers

Jeff Chivers co-founded TLATech Inc. in 2019 to build software for litigation that would dramatically improve the working lives of litigation attorneys and paralegals, and, by doing so, enable them to better and more broadly serve the administration of justice. Before launching Syllo, Jeff spent more than ten years of his career in litigation and clerked for the Honorable Pamela K. Chen of the U.S. District Court for the Eastern District of New York and for the Honorable Thomas L. Ambro of the U.S. Court of Appeals for the Third Circuit. Jeff received a J.D. magna cum laude and Order of the Coif from Georgetown University Law Center and a B.A. in Computer Science from Harvard College.

Eric Wall

Eric Wall is an Executive Vice President at Syllo. He spent more than a decade as a litigator, serving most recently as a partner at Quinn Emanuel Urquhart & Sullivan LLP, where he assisted technology companies in litigating patent disputes. Eric holds a JD from Harvard Law School and a BS in Finance from Georgetown University. He has written extensively about how generative AI will impact legal practice.

The Intersection of Psychology and Cybersecurity: Understanding Human Factors in Social Engineering

Majo Castro
Founder & Principal Attorney | CastroLand Legal

Ever wondered how our human nature affects your cyber security?

When we talk about cybersecurity, we often bring to mind firewalls, encryption, and technical defenses. **However, at the heart of many security breaches, there lies an equally critical yet frequently overlooked factor: human behavior.** Social engineering is a manipulation technique often used to exploit human psychology and gain unauthorized access to private information, by often bypassing even the most robust security systems. Attackers manipulate cognitive biases, behavioral patterns, and emotional responses in order to deceive individuals. In other words, cybersecurity is not just a technological issue, but a deeply human one.

The Psychology Behind Social Engineering Attacks

As Dr. Seth Nielson, president of Crimson Vista, explains in his book Discovering Cybersecurity, social engineering attacks thrive on the manipulation of human nature at their core. Cyber attackers rely on understanding and exploiting psychological principles, including trust, authority, and reciprocity, to trick victims into revealing sensitive information or taking actions that can compromise their cyber security.

Cognitive Biases: Flaws in Human Judgment

Our brains often take shortcuts when we are making decisions that are often made, and sometimes, those shortcuts will lead us straight into a security trap. Mental habits like these are known as cognitive biases, and can often cloud our logical judgement. Hackers know this and they often use known cognitive biases to their advantage. They trick people into making risky uninformed decisions.

Cognitive biases are systematic patterns of deviation from rational judgment. Attackers leverage these biases to manipulate individuals into making poor security decisions. Some key biases that social engineers exploit include:

1. Authority Bias: People are more likely to comply with requests from perceived authority figures. Attackers often pose as executives, law enforcement, or IT support to gain trust.
2. Urgency and Scarcity: Creating a false sense of urgency (e.g., "Your account is compromised! Act now!") to pressure individuals into making hasty decisions.
3. Reciprocity Principle: If an attacker offers something of value (e.g., free software, a helpful guide), a potential victim may feel obligated to return the favor, often by sharing sensitive data.
4. Overconfidence Bias: Many people believe they are too smart to be tricked, making them more susceptible to sophisticated attacks.

Emotional Triggers and Visual Manipulation in Phishing Attacks

Emotions play a significant role in decision-making, and attackers exploit this through fear, curiosity, excitement, or even guilt. Phishing emails often use alarming messages (e.g., "Your bank account has been locked!") or visual cues like urgent red warnings to induce panic and prompt immediate action. The interplay of color, design, and urgency creates a psychological response that overrides

rational judgment, making individuals more likely to click malicious links or provide confidential information.

The Five Stages of Ignorance in Security Awareness

Phillip Armour's "Five Stages of Ignorance" framework applies directly to cybersecurity awareness and the dangers of social engineering:

1. Lack of Awareness: Users don't know that threats exist (e.g., believing phishing emails are rare).
2. Lack of Understanding: Users recognize threats but don't understand how they work (e.g., assuming only "obvious scams" are dangerous).
3. Lack of Process Knowledge: Users understand the threats but don't know how to defend against them effectively (e.g., failing to use password managers or multi-factor authentication).
4. Lack of Skill: Users know the defense strategies but lack the experience to apply them consistently (e.g., failing to spot subtle phishing attempts).
5. Lack of Adaptation: Users rely on outdated knowledge, unaware that attacks evolve (e.g., thinking all phishing attempts contain grammatical errors).

Addressing these stages through continuous education and adaptive security measures is essential to mitigating social engineering risks.

Sources of Error in Cybersecurity Decision-Making

Mistakes in cybersecurity often stem from predictable sources of error:

- Perception Errors Users misjudge risks, assuming a well-designed email must be legitimate.
- Memory Errors: Forgetting to update passwords or reuse credentials across multiple sites.
- Decision Errors: Clicking on links impulsively due to stress, urgency, or misplaced trust.
- Execution Errors: Entering sensitive information into the wrong site due to distractions.

Digital Behavior, Privacy, and Security Risks

Online behaviors create a digital footprint, which attackers can exploit. There are two main types:

- Active Digital Footprint: Includes social media posts, search queries, and online purchases. Attackers use use this information for spear phishing or identity theft.
- Passive Digital Footprint: Data collected without direct user input, such as tracking cookies, IP addresses, or metadata from apps. This data helps attackers profile targets and predict behavior.

Behavioral patterns in apps and online transactions can reveal security weaknesses. For example, frequent logins from multiple locations may indicate compromised credentials. Understanding these patterns helps users minimize exposure by adjusting privacy settings, using VPNs, and limiting personal data sharing.

Psychology-Aware Design: Creating Security-Conscious Interfaces

Cybersecurity must not be only relied on user vigilance but also incorporate psychology-aware design to mitigate risks. Some key principles include:

- Reducing Cognitive Load: Simplifying security processes to prevent decision fatigue.
- Behavioral Nudging: Encouraging safer choices through subtle interface cues, such as warning messages before sharing sensitive data.
- Default Security Settings: Enforcing strong passwords and multi-factor authentication by default, rather than as optional features.

Actionable Takeaways - Strengthening Security Through Awareness

To protect against social engineering attacks and digital privacy risks, individuals and organizations should adopt these best practices:

1. Pause Before Acting: If a message creates urgency, stop and verify its authenticity before responding.
2. Verify Sources: Double-check URLs, email senders, and request legitimacy before sharing sensitive data.
3. Use Multi-Factor Authentication (MFA): Even if passwords are compromised, MFA adds an extra layer of protection.
4. Be Mindful of Digital Footprints: Regularly review privacy settings, limit data sharing, and use encrypted communications when possible.
5. Participate in Security Drills: Organizations should conduct regular phishing simulations and training to improve response readiness.
6. Encourage a Security-Conscious Culture: Open

discussions about cybersecurity make it easier for employees and individuals to spot and report threats.

Conclusion: Cybersecurity Is a also a Human Challenge

As technology gets more woven into our everyday lives, it's super important to understand the psychological side of cybersecurity. Hackers often play on our cognitive biases, emotions, and online habits to trick us. By being aware of these tactics and using security practices that take psychology into account, we can really reduce our risks. Cybersecurity isn't just about firewalls and encryption; it's also about understanding how people think and making smart choices to protect our privacy and security in this increasingly complex digital world.

ABOUT THE AUTHOR:

Majo is the founder and principal attorney of CastroLand Legal, combining advanced legal expertise with firsthand business experience. She holds an LL.M. in Cybersecurity Law from the University of Texas, specializing in data privacy, cybersecurity, and emerging technologies.

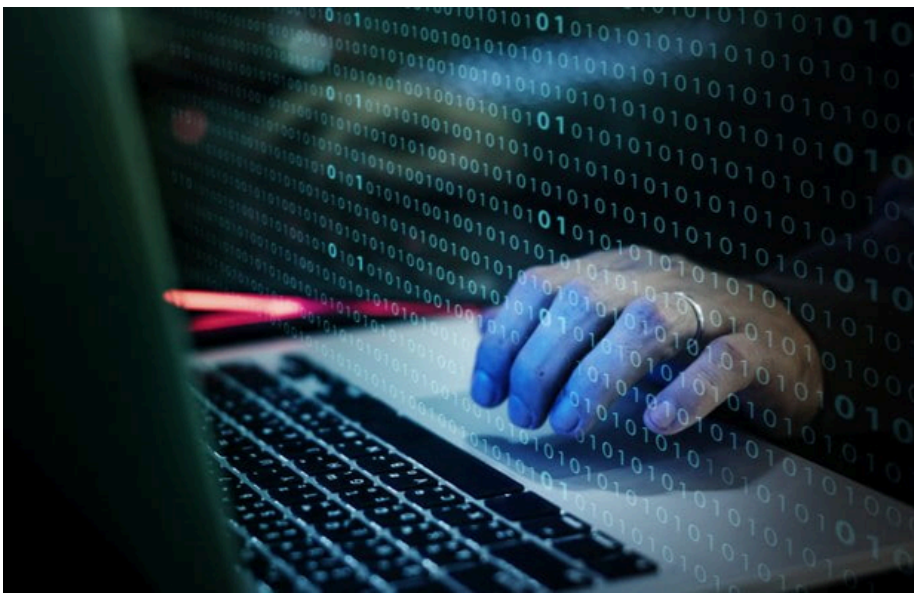
Majo and her team are dedicated to helping businesses navigate complex legal landscapes with practical, proactive solutions. CastroLand Legal strives to be a trusted partner in cybersecurity, compliance, and business law, delivering modern, ethical, and personalized legal support.

Expansion and Retraction: Recent Developments in the Scope of Civil CFAA Litigation

Colleen Garcia

On September 4, 2020, Irish airline company Ryanair filed suit against five online travel agents (OTAs)—Booking.com, Priceline.com LLC, Agoda Company Pte. Ltd., Kayak Software Corporation, and Booking Holdings, Inc. Ryanair alleged that the OTAs had violated the Computer Fraud and Abuse Act (CFAA) by scraping its website without authorization.

A jury trial against Booking.com commenced in the District of Delaware on July 15, 2024, and the jury returned a verdict in Ryanair's favor on July 19, 2024.[1] However, in a recent ruling on January 22, 2025, the court set aside the verdict and granted Booking.com's motion for judgment as a matter of law. The court's ruling provides helpful guidance following one of the few jury trials in the civil CFAA context.



Extraterritoriality

"The CFAA prohibits acts of computer trespass by those who are not authorized users or who exceed authorized use."[2]

Multiple courts have held that the CFAA applies extraterritorially in both criminal and civil cases.[3] They have concluded that "the text of the CFAA provides a clear indication of extraterritorial application" that is sufficient to rebut the presumption against extraterritoriality.[4]

In the recent Ryanair v. Booking.com BV ruling, the court agreed and drew

[1] On June 26, 2024, Ryanair dismissed all other defendants from the case.

[2] Ryanair DAC v. Expedia Inc., Case No. C17-1789RSL, 2 (W.D. Wash. Aug. 6, 2018) (quoting Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1065 (9th Cir. 2016)).

[3] In re Apple Inc. Device Performance Litigl, 347 F. Supp. 3d 434, 448-49 (N.D. Cal. 2018) (citing Ryanair DAC v. Expedia Inc., No. 17-CV-01789-RSL, 2018 WL 3727599, at *2 (W.D. Wash. Aug. 6, 2018); Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247 at 265, 130 S.Ct. 2869, 177 L.Ed.2d 535 (2010)); United States v. Gasperini, 729 F. App'x 112, 114 (2d Cir. 2018) ("There is a strong argument that § 1030(a)(2) applies extraterritorially."); United States v. Ivanov, 175 F.Supp.2d 367, 375 (D. Conn. 2001) (holding that Congress has "clearly manifested its intention" to apply the CFAA extraterritorially)."

[4] In re Apple Inc. Device Performance Litigl, 347 F. Supp. 3d 434, 448 (N.D. Cal. 2018)

support for extraterritorial application from both the definition of "protected computer" and the definition of "governmental entity."

The court noted that "[u]nder the CFAA, a "protected computer is a computer "which is used in or affecting interstate or foreign commerce or communication, **including a computer located outside the United States** that is used in a manner that affects interstate or foreign commerce or communication of the United States."[5] Also, a "governmental entity" "includes the Government of the United States, any State or political subdivision of the United States, **any foreign country, and any state, province, municipality, or other political subdivision of a foreign country."** (emphasis added) [6]Thus, the court held that, consistent with rulings in other cases, the plain text of the CFAA supports extraterritorial application.

However, the Booking.com case presented a new wrinkle to extraterritorial application—at trial, both parties were foreign companies. Booking.com argued that it was entitled to judgment as a matter of law because after the U.S. defendants were dismissed from the case, "'Ryanair's case at trial was reduced to a dispute between two European companies over flights solely offered in Europe and North Africa, booked exclusively through a European third-party vendor that was not a party to the litigation….'"[7]

The court disagreed. Booking.com had presented "no justification" for departing from the plain text of the CFAA.[8] Moreover, "[t]he question whether a particular extraterritorial statute applies to particular foreign activities depends on the limits that Congress has imposed on the statute's foreign application."[9] With the CFAA, it "applies only if the computer in question is one whose use affects interstate or foreign commerce."[10] For these reasons, the court held that extraterritorial application remained appropriate.

In doing so, the court's ruling made way for future civil CFAA cases involving solely foreign entities and foreign computers, so long as they are "used in a manner that affects interstate or foreign commerce or communication of the United States."[11]

Calculation of Damages

The Booking.com ruling is also notable for the court's conclusions regarding damages in civil CFAA cases.

A civil CFAA action "'may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of the subsection (c)(4)(A)(i).'"[12] At issue in the Booking.com case was subclause (I), which requires a showing of "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."[13]

[1] 18 U.S.C. § 1030(c)(4)(A)(i)(I).

At trial, Ryanair claimed approximately $177,000 in total losses during the period of March 1, 2022 to February 28, 2023.[14] Ryanair put on evidence regarding the costs of online verification, customer service agents, hosting a bot blocking program, and payments to a passenger service system company. The jury found that Ryanair had met its burden of proving loss of at least $5,000 and awarded exactly $5,000 in actual economic harm.[15]

Following the trial, Booking.com argued that the evidence presented at trial was "'entirely speculative, and by any reasonable calculation totaled-at most-$2,457.72.'"[16]

---

[5] Ryanair DAC v. Booking.Com B.V., Civil Action 20-1191-WCB, 9 (D. Del. Jan. 22, 2025) (quoting 18 U.S.C. § 1030(e)(2)(B) (emphasis added)).
[6] Id. (citing Ivanov, 175 F.Supp.2d at 374 (referring to 18 U.S.C. § 1030(e)(9)).
[7] Id. at 10.
[8] Id. at 13.
[9] Id. at 14 (citing Abitron Austria GmbH v. Hetronic Int'l, Inc., 600 U.S. 412, 418 (2023).
[10] Id.
[11] 18 U.S.C. § 1030(e)(2)(B)
[12] Ryanair DAC v. Booking.Com B.V. at 15.
[13] 18 U.S.C. § 1030(c)(4)(A)(i)(I).
[14] Ryanair DAC v. Booking.Com B.V., at 16.
[15] Id. at 5, 17.
[16] Id. at 17.

In reviewing the evidence, the court first noted that the definition of "loss" in the CFAA "'focus[es] on technological harms.'"[17] Further, the jury was instructed that "[l]osses do not include any costs that are not borne by Ryanair."[18]

Regarding the online verification costs, the "undisputed evidence" at trial demonstrated that "those costs were passed on to the customers."[19] "Ryanair d[id] not point to any evidence from which the jury could conclude that Ryanair's online verification process could have resulted in a loss for Ryanair."[20]

On the cost of customer service agents, Ryanair presented no evidence at trial of which customer service agent costs were specifically attributable Booking.com.[21] Moreover, Ryanair did not explain what portion of the customer service agent costs related to "technological harm" caused by web scraping without authorization, as opposed to other bases for customer complaints.[22]

Similarly, the court held that Ryanair's passenger service system costs could not be considered a "loss" under the CFAA because they were not directed to any technological harm.[23] The system was a "backing database that store[d] all of [Ryanair's] flight bookings." There was "no special fee" for storing OTA bookings as opposed to other bookings, so Ryanair paid the same amount, "no matter how the flight [wa]s booked."[24]

The only arguable "loss" to Ryanair under the CFAA was the cost to host its bot blocking program. However, of the 80% of the hosting costs associated with the relevant portion of Ryanair's website, only 2.8% of those costs were attributable to Booking.com.[25] Considering only the hosting cost data presented at trial (and excluding "impermissible extrapolations"), "the non-speculative evidence support[ed], at most, a finding of $2,457.72" during the relevant one-year period.[26]

Therefore, Ryanair did not meet its burden of proving a "loss" of at least $5,000 in a one-year period, and the court granted Booking.com's judgment as a matter of law.

Conclusion

Whether or not the court's ruling in Booking.com will stand remains to be seen. If so, civil CFAA litigators and scholars should prepare for both increasingly non-U.S. application and also heightened scrutiny of damages calculations.

ABOUT THE AUTHOR:

Colleen García is a graduate of Georgetown University's Walsh School of Foreign Service, the Naval Postgraduate School of International Graduate Studies, and Columbia Law School, where she was a Harlan Fiske Stone Scholar and Articles Editor of the Columbia Law Review. After graduation, Colleen clerked for Chief Justice Wallace B. Jefferson and Justice Jeffrey V. Brown, of the Supreme Court of Texas. She then began work as an Attorney Advisor for the Department of Justice National Security Division, during which time she served as Director for Cybersecurity Policy for the National Security Council Cybersecurity Directorate. She then served as an Assistant United States Attorney in the National Security and International Crimes Unit of the Eastern District of Virginia, where she prosecuted terrorism, espionage, and cybercrimes. She returned to her home state of Texas in 2019, where she continues working on cybersecurity and data privacy matters in private practice.

[17] Id. at 16 (quoting Van Buren v. United States, 593 U.S. 374, 392 (2021)).
[18] Id. at 16.
[19] Id. at 21.
[20] Id.
[21] Id. at 22.
[22] Id. at 23–24.
[23] Id. at 32–33.
[24] Id. at 31, 33.
[25] Id. at 27.
[26] Id. at 31.

The Tariff Man: What to Expect from Trump's Second Term

Since President Trump was elected on November 6, 2024, many have been hypothesizing what would become of U.S. trade policy during his second term. During his campaign, and since his win in November, Trump has made several promises concerning trade policy. He promised that on his first day in office, he would sign an Executive Order that would put in place a 25% tariff on all imports of goods coming from Canada and Mexico.[1] He also stated he would place a 60% tariff on all products from China.[2]

So, it should come as no surprise to anyone that Trump's trade policy for the next four years will utilize tariffs. On January 2, 2025, President Trump tweeted "The Tariffs, and Tariffs alone, created this vast wealth for our Country…Tariffs will pay off our debt and, MAKE AMERICA WEALTHY AGAIN!"[3]

The question is, will Trump enact tariffs tailored to specific industries and commodities deemed important to American security and economy as the Biden Administration did when increasing tariffs on electric vehicles, batteries, semiconductors, and other products from China in 2024[4], or will he use them more broadly?

The answer to this question is unclear at the moment. Trump called a Washington Post article, citing sources claiming Trump's aides were exploring a narrower approach to tariffs, focused on certain critical sectors, "fake news."[5] However, on the first day of his presidency, President Trump published a memorandum, titled "America First Trade Policy," outlining his administration's trade policy plan, which seemed to signal a more measured approach to tariffs than the promises made during his campaign.[6] But just three weeks into his presidency, we see his use of tariffs against China, Canada, and Mexico used broadly.

President Trump signed three Executive Orders on February 1, 2025, imposing an additional 10% tariff on all products from China and an additional 25% tariff on all products from Canada and Mexico. The 25% tariffs on Canada and Mexico were paused and will not take effect until March 4, 2025.[7]

Whether he takes a narrow or comprehensive approach going forward, the technology sector, which is considered a major contributor to the U.S. trade deficit with China, should be prepared.[8]

America First Trade Policy

The "America First Trade Policy" memorandum provides a plan for the Trump Administration to assess current trade policy effectiveness before determi-

ning the best policy actions for the American economy, American workers, and national security. Some policies "narrowly" target China's policies, which were subject to the United States Trade Representative's (USTR) Section 301 investigation, the steel and aluminum industries, and connected vehicles, but other policies illustrate a willingness to use tariffs against China and others comprehensively.

The most significant policy priorities within the "American First Trade Policy" memorandum are:

1. *Determining whether a* **"global supplemental tariff"** *can address the U.S. trade deficit.*
This could mean an additional tariff on all goods coming from any country. The memorandum does not provide any insight into whether goods coming from countries the U.S. currently has Free Trade Agreements (FTAs) with will be subject to the global supplement tariff if implemented.

2. Assessment of China's policies related to technology transfer, intellectual property, and innovation, policies which were investigated by the U.S. and addressed by imposing Section 301 duties on Chinese goods in 2019. The assessment should determine whether there is a need for additional tariffs or measures to address circumvention through third countries. The Biden Administration addressed the circumvention of Anti-Dumping and Countervailing duties (AD/CVD) on solar cells from China. The circumvention order targeted solar panels from Vietnam, Cambodia, Malaysia, and Thailand made with specific Chinese components.[9]

This circumvention order eliminated the need for a substantial transformation analysis. Substantial transformation is the legal principle used to determine the country of origin (COO) of a product for purposes of trade remedy application, such as Section 301 and AD/CVD duties. The COO of a product is the country where the product undergoes extensive processing and manufacturing operations. Relying on substantial transformation, companies could continue to source components from China, as long as they underwent necessary operations which would fundamentally alter, i.e., substantially transform them in other countries, without paying trade remedy tariffs.

Technology companies that sought to make changes to their supply chains to seek relief from Section 301 duties or AD/CVD duties and moved operations to other countries, such as Thailand, Taiwan, or Vietnam, should be attentive to announcements of circumvention measures or additional tariffs on Southeast Asian countries.[10]

3. *Review and assessment of the effectiveness of existing Section 232 measures on steel and aluminum and recommend adjustments.*
President Trump has expressed his intention to protect domestic steel and aluminum industries.On January 27, 2025, he announced his intention to place tariffs on steel, aluminum, and copper imported to the U.S., as well as goods such as computer chips and semiconductors, to increase U.S. production of the products.

Additionally, on December 1, 2024, the Steel Manufacturers Association (SMA), a major steel industry group in the United States, presented a "5-Point Action Plan" to President Trump.[11] The Action Plan's requests to President Trump that may impact the U.S. technology industry are:

- Include downstream products made of steel in the list of steel articles covered by Section 232.
- Increase Section 301 tariffs to 60% on steel-intensive downstream products.
- Apply Section 301 on any Chinese-origin products that are further processed or incorporated into downstream products in third countries.

The President has not publicly made comments about the specific policy requests made by the SMA. However, the President signed Executive Orders on February 10, 2025, and February 11, 2025, which seem to respond to some complaints from the steel industry. Notably, the Executive Orders, which take effect on March 12, 2025:[12]

- Impose a 25% Section 232 duty on imports of steel and derivatives from previously exempt countries, which include, Argentina, Australia, Brazil, Canada, the EU, Japan, Mexico, South Korea, the UK, and Ukraine.
- Increase the 10% Section 232

- duty on imports of aluminum and derivatives to 25%, which will be imposed on previously exempt countries, including Argentina, Australia, Mexico, Canada, the EU, and the UK.
- Impose 25% duties on additional derivative steel and aluminum articles to be published in a Federal Register notice.
- Instruct the Department of Commerce (DOC) to create a process for including additional derivative steel and aluminum articles.

The Executive Order instructs the DOC to include in the additional derivative process an avenue for domestic producers of steel and aluminum articles or derivative steel and aluminum articles, or an industry association representing one or more such producers, to request that specific derivative steel and aluminum articles be included within the scope of the Section 232 duties. Currently, steel and aluminum derivative products are wires, cables, bumper stamping, nails, tacks, etc.

The SMA specifically listed fabricated structural steel and prestressed concrete strands as derivative articles which were evading Section 232 duties in its plan. Manufacturers and companies who import fabricated steel and aluminum products should stay vigilant of derivative articles included in the scope of Section 232 duties. Automotive, aerospace, heavy machinery, laptops, and cell phone parts could be affected by the inclusion of certain steel and aluminum-intensive downstream products.

The Executive Order also instructs Customs and Border Protection (CBP) to prioritize reviews of steel and aluminum imports and to penalize violations at the maximum amount.

4. *Assessment and recommendation of* **China's Normal Trade Relations (NTR) status.**

Revoking China's NTR status would mean that the U.S. could tariff Chinese goods with impunity and without the legal authority of trade remedies such as Section 301 and Section 232. Countries currently without NTR status in the U.S. are Cuba, North Korea, Russia, and Belarus.

5. *Review and recommend appropriate action with respect to the rulemaking by the Office of Information and Communication Technology and Services (OICTS) on connected vehicles and consider whether controls on ICTS transactions should be expanded to account for additional connected products.*

The OICTS is responsible for implementing the Information and Communications Technology and Services (ICTS) Program for the Department of Commerce. The OICTS is tasked with identifying and addressing potential risks within the ICT supply chain, including hardware, software, and services, that could pose a security risk to the U.S.

On January 16, 2024, OICTS published a rule prohibiting certain transactions involving the import or sale of connected vehicles and certain hardware and software with a sufficient nexus to China or Russia. [13]

Importers of connected products should monitor rules from the OICTS, as additional connected products could include headphones, smart watches, smart appliances, security cameras, motion sensors, and any other products that connect to the internet.[14]

A Possibly Unsatisfactory Conclusion

Initially, the "America First Trade Policy" memorandum seems to indicate that President Trump would enact comparatively measured trade policy changes, but just three weeks into his presidency, he has begun making good on his campaign promises by implementing tariffs on China, Canada, and Mexico. Additionally, on January 26, 2025, Trump threatened 25% tariffs on all goods from Colombia immediately after the Colombian President barred two planes carrying deported migrants from entering his country.[15] At first, Colombia threatened retaliation but later reversed its decision and agreed to accept the migrants.

Some argue that President Trump is just a fan of hyperbole for the sake of negotiation; however, it is for this reason that the trade community cannot possibly foresee all trade policy actions from the Trump Administration. We know the self-proclaimed Tariff Man will utilize tariffs and other barriers to trade against China and countries he sees as nuclei of circumvention. However, we do not know with

certainty if President Trump will apply tariffs in an effort to pressure foreign governments to acquiesce to U.S. foreign policy.

It is also important to note that China, the largest exporter in the world, and the second largest importer of the world, after the U.S., is also engaging President Trump and the U.S. in this "trade war," and has been since 2018.[16] On February 4, 2025, China announced retaliatory tariffs on American imports of coal, liquefied natural gas, crude oil, agricultural machinery, and large-engine cars.[17]

However, the Chinese approach to this "trade war" is different. China, while using tariffs and non-tariff barriers to trade on the U.S., has simultaneously opened up its market to other countries. In 2024, China eliminated tariffs on goods coming from 33 of the world's least developed countries,[18] continued to strengthen economic ties with Russia,[19] and updated Free Trade Agreements with Peru and the Association of Southeast Asian Nations (ASEAN).[20]

China is also considering unilateral trade incentives to U.S. ally countries in response to the Trump Administration. A strategy that some have labeled "unilateral opening," may mean tariff cuts to incentivize more trade with Europe and other Asian countries.[21] This may increase the competition to U.S. technology in the Chinese market.

This strategy is in stark contrast to the approach by the Trump Administration, who has looming tariffs on Canada and Mexico in March and has threatened the EU with its own "trade war."[22]

U.S. technology companies, especially those with large U.S. and Chinese markets, should continue to diversify their supply chains, reorganize supply chains to reduce cross-border dependency, leverage Free Trade Agreements and duty-saving programs, and closely monitor trade policy changes in both countries.

ABOUT THE AUTHORS

Marina Mekheil

Senior Associate

Formerly with the U.S. Customs and Border Protection (CBP) Headquarters, Marina is a Senior Associate at Schulz Trade Law PLLC. She advises her clients on various trade issues, including matters relating to customs, sanctions, and export controls. She predominantly assists clients with customs issues, advising clients on classification, valuation, trade remedies, and Free Trade Agreements (FTAs). While at Schulz Trade Law PLLC, Marina has worked on various import and export law matters. She has assisted clients in identifying and disclosing discrepancies in import activities to CBP in Prior Disclosures, while minimizing potential liabilities and ensuring regulatory compliance. Additionally, she has effectively represented clients facing large penalties from CBP, resulting in substantial penalty reductions. Her understanding of complex customs issues has resulted in successful ruling requests and protest filing on behalf of her clients. Prior to joining Schulz Trade Law PLLC, Marina began her career as an attorney with CBP's Office of Trade, Regulations and Rulings Directorate, where she advised the U.S. Government on customs matters concerning advanced rulings, litigation proceedings, and customs law trainings. Additionally, while attending law school in the District of Columbia, Marina interned at various federal agencies, including the U.S. Trade Representative (USTR) and the Department of Commerce. These experiences have allowed Marina to provide her clients with comprehensive legal advice. In her free time, Marina enjoys traveling and playing pickleball.

NOTE FROM AUTHORS:
This article was drafted on February 12, 2025, and does not include an analysis of events or government actions which occurred between February 12, 2025, and the date this article was published,

Matt Savage

Senior Trade Analyst

Matt Savage is a Senior Trade Analyst with over 25 years of experience in international trade compliance. He has done extensive work in U.S. trade regulations for various freight forwarders, customs brokers, importers, and exporters. As a seasoned trade professional, he brings a depth of industry knowledge that translates to practical client oriented solutions. Matt has devoted his career to helping clients navigate the intricacies of U.S. trade compliance programs. Using his unique experience, Matt provides strategic solutions for trade compliance concerns. This often involves helping clients identify compliance gaps in areas like international supply chain, procurement support, and global logistics. He also works with a wide array of industries, including oil and gas, cosmetics, manufacturing, aerospace, telecommunications, and software. Matt regularly consults clients on matters related to regulatory compliance in disclosures, audits, valuations, assists, procurement, Free Trade Agreements (FTAs), USMCA origin analysis, import and export documentation and recordkeeping requirements, and classification determinations (HTS, ECCN, and ITAR). He also leverages his prior experience as a certified internal ISO auditor and a Lean/Six Sigma Green Belt to assist clients develop procedure and process efficiencies in their trade compliance programs.

Optimizing Sales and Onboarding: Maximizing Technology to Streamline Your Workflow

Ruby L. Powers

In today's fast-paced world, client expectations are higher than ever. Clients demand efficiency, transparency, and seamless interactions from start to finish. For legal practices, optimizing sales and client onboarding processes are no longer optional; they need to be done to stay competitive. Technology offers tools and strategies to revolutionize these workflows, reducing friction, enhancing client satisfaction, and boosting overall efficiency.

The Role of Technology in Sales and Onboarding

Tools like customer relationship management (CRM) systems can automate repetitive tasks, such as sending follow-up emails or tracking client interactions. By connecting sales and onboarding workflows through integrated platforms, law firms can ensure a seamless transition from prospect to client. Artificial Intelligence (AI) and data analytics allow for tailored communication, ensuring clients feel understood and valued throughout their journey.

Implementing Technology to Streamline Sales

Centralized CRM tools like **Lawmatics**, allow law firms to efficiently track leads, automate reminders, and measure sales performance. These platforms ensure no potential client slips through the cracks and provide actionable insights for improving conversion rates.

AI-powered tools can analyze lead behavior and predict which prospects are most likely to convert. This enables law firms to focus their efforts on high-priority leads, maximizing their chances of success. Timely and personalized follow-ups are critical to closing new business. AI-driven tools can automate email sequences, text reminders, and appointment scheduling, ensuring that potential clients stay engaged throughout the decision-making process. Automated email sequences and chatbots can keep prospects engaged and informed, answering common questions instantly while freeing up time for your team to handle more complex inquiries. Chatbots and virtual assistants can handle initial inquiries, schedule consultations, and even provide basic case information, reducing administrative burden while maintaining client engagement.

By using AI-powered tools that analyze intake forms, prior case outcomes, or industry trends, attorneys can approach consultations better prepared, increasing the likelihood of client retention. Automated data collection and document review ensure that attorneys spend less time gathering information and more time strategizing.

Modern law firms can use data analytics and AI-driven reporting to refine their sales approach. Tracking key performance indicators (KPIs) such as conversion rates, response times, and client engagement trends helps firms adjust their strategies for better results. Tools like Google Analytics, Clio Grow, or Salesforce provide real-time insights that empower firms to make informed decisions about marketing, outreach, and sales tactics.

Streamlining Client Onboarding with Technology

Tools such as DocuSign and Clio Grow simplify the collection and sharing of documents, enabling clients to complete paperwork quickly and securely from any device.

A centralized client portal allows clients to access updates, share documents, and communicate with your team in one secure location. This transparency builds trust and reduces the back-and-forth often associated with onboarding. Intelligent forms and automated data entry tools streamline the client intake process, reducing errors and saving valuable time for both clients and staff. These

features can be included in your CRM purchase.

Project management tools like Trello and Asana can help assign onboarding tasks to team members, track progress in real-time, and ensure deadlines are met without oversight slipping through the cracks.

Reducing Friction and Improving Client Satisfaction

Tools that keep clients informed throughout the onboarding process help build trust and eliminate confusion. Faster processing times ensure clients feel their time is respected, improving satisfaction and retention. Self-service options, such as online scheduling and digital forms, allow clients to engage with your practice on their terms, fostering convenience and loyalty.

Automated status updates and client portals provide real-time visibility into the progress of their case or engagement, reducing the need for repeated follow-up inquiries. AI-powered chatbots and virtual assistants can provide instant responses to common questions, guiding clients through each stage of onboarding without requiring staff intervention. This reduces bottlenecks and ensures that clients receive prompt, consistent communication at every touchpoint.

A frictionless onboarding experience translates to higher client satisfaction, improved retention rates, and increased referrals. When clients feel valued and supported from the outset, they are more likely to have a positive perception of your firm, enhancing both reputation and long-term success.

Metrics to Measure Success

Monitor lead conversion rates, response times, and the average time to close deals. Measure the time it takes to onboard clients, client satisfaction scores, and the reduction of errors in documentation. Measure the percentage of prospective clients who move from initial inquiry to signed engagement. A high conversion rate indicates that your sales process, follow-ups, and technology-driven onboarding are effectively guiding clients through the decision-making process.

Evaluate the cost of technology tools against their impact on workflow efficiency and client retention. Compare the cost of automation tools, CRMs, and AI-driven solutions against their impact on client conversion, efficiency, and revenue growth. A strong ROI justifies continued investment in technology.

Track how quickly your firm responds to inquiries, consultation requests, and client messages. Faster response times often correlate with higher client satisfaction and increased conversion rates. Use surveys or automated feedback tools to gauge how satisfied clients are with the onboarding experience. Happy clients are more likely to refer others, improving your firm's reputation and client acquisition.

Tips for Successful Technology Adoption

Assess the specific challenges your practice faces in sales and onboarding before choosing tools. Not every solution will fit every practice. Ensure everyone understands how to use new technology effectively. A well-trained team is key to maximizing the benefits of tech investments. Begin with one or two critical tools, such as a CRM or document management system, and expand as needed. Technology evolves rapidly. Periodically assess your tools and workflows to ensure they continue to meet your needs.

Conclusion

Optimizing sales and onboarding with technology is a game-changer for modern practices. By addressing pain points, automating repetitive tasks, and focusing on client-centric innovation, firms can reduce friction, enhance client satisfaction, and boost overall efficiency. The tools are out there; the key is to start small, stay curious, and embrace the potential of technology to transform your practice.

ABOUT THE AUTHOR:

Ruby L. Powers, a Board Certified immigration attorney and founder of Powers Law Group, P.C., has over 16 years of expertise in law practice management. Author of AILA's Build and Manage Your Successful Immigration Law Practice (Without Losing Your Mind) and Power Up Your Practice: Create the Law Firm and the Life You Deserve, available on Amazon.com. Ruby shares invaluable knowledge on law practice management and small business consulting. Through Powers Strategy Group, LLC, she provides strategic consulting services and hosts the informative podcast "Power Up Your Practice". With a commitment to excellence and empowerment, Ruby inspires legal professionals to succeed in their practices and businesses.

Authorities cannot view hash-trapped files without a warrant.

Pierre Grosdidier

In United States v. Maher, the Second Circuit Court of Appeals joined its sister the Ninth Circuit Court of Appeals in holding that authorities cannot view hash-trapped files suspected of featuring sexually abused children without a warrant.

In United States v. Maher, the Second Circuit Court of Appeals joined its sister the Ninth Circuit Court of Appeals in holding that authorities cannot view hash-trapped files suspected of featuring sexually abused children without a warrant.[1] It nonetheless upheld Ryan Maher's conviction for possession of child pornography on basis of the good faith exception to the exclusionary rule because authorities had a good faith reason to believe that they could review Maher's hash-trapped contraband image without a warrant.[2]

Google uses a hash-value filter to detect contraband images.[3] Dedicated Google staff have built and now maintain a repository of hash values of these images (Google discards the images after adding their hash values to its repository).The hash values of images that pass through Google servers are automatically compared to those in the repository. Google reports trapped contraband images, i.e., images that are found to have a matching hash value in the repository, to the National Center for Missing and Exploited Children (NCMEC) along with the corresponding email accounts information. NCMEC staff then work with local authorities to identify, arrest, and prosecute the alleged wrongdoers.[4]

Google employees sometimes review the trapped images to confirm their illicit nature but, as in Maher's case, these images are also often automatically reported uninspected to the NCMEC as "apparent child pornography." A New York State police investigator eventually reviewed one trapped image from one of Maher's gmail accounts without a warrant. This review confirmed the image as contraband. Authorities then secured warrants to search Maher's gmail accounts and his residence where they found troves of contraband, including a copy of the trapped image. At trial, Maher argued that authorities conducted a warrantless search of the trapped image. The trial court denied the motion based on the private search doctrine and the good faith exception. It held that authorities had not exceeded Google's private search of the trapped file because the hash value algorithm made it virtually certain that the investigator would see the same contraband that a Google employee saw when it created the image's hash value.[5]

The Second Circuit Court of Appeals disagreed that no Fourth Amendment violation occurred. It reiterated that the private search doctrine applies only when the scope of a warrantless police search does not exceed that of a private party. Thus, authorities violated the Fourth Amendment when they viewed movie reels on a projector after a private party first tried to see "'portions' of one of the suspect films 'by holding it up to the light.'"[6]

---

[1] 120 F.4th 297, 301 (2d Cir. 2024); see also United States v. Wilson, 13 F.4th 961 (9th Cir. 2021); but see United States v. Reddick, 900 F.3d 636 (5th Cir. 2018) (no expectation of privacy in hash-trapped files).
[2] Maher, 120 F.4th at 301–02.
[3] See Pierre Grosdidier, Hash values and the Fourth Amendment, Circuits, Mar. 2021, p. 49.
[4] Maher, 120 F.4th at 301–03.
[5] Id. at 304–05.
[6] Id. at 309–12 (quoting Walter v. United States, 447 U.S. 649, 652 (1980)).

Alternatively, authorities were free to review without a warrant documents previously searched by burglars.[7] Here, the Court distinguished between the image whose hashed value rested in Google's repository and Maher's trapped image. The two images' hash value match would have provided probable cause for a warrant to search Maher's image, but it did not allow authorities to view the latter without a warrant. At some point, someone at Google had seen the image that resulted in a saved hash value in Google's repository. But no one at Google had seen Maher's image, a different digital file.Thus, the investigator who reviewed Maher's image exceeded Google private search, which did not include physically viewing his image.[8] The investigator's search, therefore, violated the Fourth Amendment.

Nonetheless, the Court agreed that the good faith exception to the exclusionary rule applied. The rule applies when, inter alia, authorities act without a warrant "under circumstances that 'they did not reasonably know, at the time, [were] unconstitutional.'"[9] When the state investigator searched Maher's image, the only appellate case on record was United States v. Reddick, which held that a person had no expectation of privacy in hash-trapped files. United States v. Wilson, which held otherwise, was decided more than a year after the search. Under these circumstances, the investigator's belief that she could search the image without a warrant was reasonable and the good faith exception applied.[10]

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. 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, a Fellow of the Texas Bar Foundation, and a registered P.E. in Texas (inactive). He was the State Bar of Texas Computer & Technology Section Chair for 2022–23 and was elected Medium Section Representative to the State Bar of Texas for the 2023–26 term.

[7] Id. at 313 (citing United States v. Knoll, 16 F.3d 1313, 1320–21 (2d Cir. 1994)).
[8] Id. at 313–17.
[9] Id. at 320–21 (quoting United States v. Ganias, 824 F.3d 199, 221–22 (2d Cir. 2016) (en banc)).
[10] Id. at 320–22.

NIST Framework Small Business Quick Start Guide Applied for Solos

Fatima Naeem

Cybersecurity is a concern for solo attorneys managing law practices in an increasingly digital world.

Cybersecurity is a concern for solo attorneys managing law practices in an increasingly digital world. This article explores how the National Institute of Standards and Technology (NIST) framework's Small Business Quick-Start Guide[1] (The Guide) can be adapted to develop effective incident response plans for cyberattacks and data breaches. This article provides some steps you can take to begin your cybersecurity risk management strategy: Govern, Identify, Protect, Detect, Respond, and Recover. The Guide discusses various actions to consider for each of these steps. In addition, I would encourage you to review the Guide directly for more details.

1) Govern

A. UNDERSTAND:

- Evaluate the type of law you're practicing and the sensitive data involved.
- If you have a general practice, chances are you need a comprehensive cybersecurity risk management strategy in place. If you focus on Family Law, Guardianships, Probate Matters, Child Welfare Law, Healthcare Law, Mediations, Arbitrations, etc., you most likely handle clients' intimate pictures, mental health records, bank information, minor child(ren)'s protected information, HIPAA, and/or personally identifiable information. This is just to name a few.
- Assign responsibility for developing and implementing a cybersecurity strategy. As a solo attorney, you're it. Consider outsourcing to an expert before an incident occurs.

B. ASSESS:

- Analyze the impact if your or your clients' personal information was compromised.
- Evaluate whether investing in cybersecurity insurance aligns with your firm's level of risk exposure. If you have a significant amount of sensitive information, obtaining cybersecurity insurance is highly recommended.
- Ensure that contractors or third-party vendors, such as those who manage billing, have a solid cybersecurity plan in place. If they are hacked, then your client's sensitive data may also be compromised. [For solos, this is often a contracted individual managing billing tasks.]
- Incorporate cybersecurity considerations into your annual budgeting and planning to ensure adequate resources are allocated to mitigate risks. When setting your annual firm goals, consider how cybersecurity risks may impact your budget and the types of cases you plan to take on.

C. PRIORITIZE:

- If you are unsure where to start, ask for help. As attorneys, we are usually the first ones to help and the last ones to ask for it. Cybersecurity is too important not to ask.

D. COMMUNICATE:

- Develop and formalize a written cybersecurity policy or plan. A cybersecurity plan needs to be more than a mental note/a sticky note/etc. – document it and make it accessible.

2) Identify

A. UNDERSTAND:

- Identify the management system(s) you use for your client files. Google Drive, OneDrive, PracticePanther, Clio, or others? Take an inventory of all your firmware, including desktop, tablet, laptop, etc. – especially if you're using multiple (perhaps, one for court and one for day-to-day use).
- Document your technology inventory.

B. ASSESS:

- Inspect your physical and digital systems for vulnerabilities. Leaving your office door open creates opportunities for theft, just as leaving your digital systems unsecured can lead to cyberattacks.
- Don't write down your usernames and passwords and put it next to your computer.
- Implement Multi-Factor Authentication (MFA), to add an extra layer of security by requiring a second verification method. If you do not already have it, please get it as soon as possible. It is definitely worth it to have MFA if there's ever an issue.

C. PRIORITIZE:

- Classify your data into these categories depending on impact level: low, moderate, and high.[2] This is just one suggestion; there are many ways to classify your data. Do your own research and find the best fit for your own firm. All in all, keep it simple.

D. COMMUNICATE:

- Share and reinforce your cybersecurity plan with staff and third parties.
- Be open to feedback from others because they may be able to suggest solutions you've yet to encounter. Collaborate with other solo attorneys and learn about their cybersecurity practices.

3) Protect

A. UNDERSTAND:

- Restrict access to sensitive information. Think about the information you do have. Who all has access to it? Do they need access to it? If you only have one employee helping with billing, they do not need to be in the discovery section of your client's files.

B. ASSESS:

- How often are you going to brush up on your cybersecurity? (The answer is constantly. Realistically, commit to at least quarterly updates to stay ahead of emerging threats).
- Invest in ongoing training for yourself and your staff to ensure awareness and preparedness. It is worth the time and money in the long run.

C. PRIORITIZE:

- Do not use one password for everything.
- Strengthen your passwords and consider using a secure password manager to store them.

D. COMMUNICATE:

- Be cautious of suspicious activity or irregularities. If something seems suspicious, it likely warrants further investigation. Do not click on it.
- Educate your staff on recognizing and reporting phishing scams.
- Report suspicious activity to peers in your professional groups, like the Texas Lawyers' Facebook groups to raise awareness and prevent widespread impact. Do not provide your client's confidential details.

4) Detect:

A. UNDERSTAND:

- Recognize warning signs of a cybersecurity breach. For example, if you get multiple failed login attempts – take appropriate action.

B. ASSESS:

- Investigate anomalies in your system. If you start seeing an app open on your computer that you do not recognize, investigate further. Do not click on it. Research separately what the app might be.

C. PRIORITIZE:

- Install and maintain anti-virus and anti-malware software for all your electronic devices.

D. COMMUNICATE:

- If you decided to contract your cybersecurity with a third party, be sure to let them know as soon as you think something is off. (Personally, when it comes to cybersecurity, it's better to be known as the attorney

- who cried wolf reporting everything suspicious than someone in trouble because they did nothing.)
- Engage a trusted IT or cybersecurity professional if you suspect an issue.

5) Respond

A. UNDERSTAND:

- Prepare a response plan that includes immediate steps.
- Where is the plan located? Who are you going to call? Do you need to report to someone? What about a court coordinator? Other attorneys?

B. ASSESS:

- If a cybersecurity incident does occur, take a moment to steady yourself. Panic for about 5 seconds, then breathe for 10 seconds. Now, onto action.
- Categorize the breach (low, medium, or high risk), what happened, how did it happen?

C. PRIORITIZE:

- If a cybersecurity incident does occur, take a moment to steady yourself. Panic for about 5 seconds, then breathe for 10 seconds. Now, onto action.
- Categorize the breach (low, medium, or high risk), what happened, how did it happen?

D. COMMUNICATE:

- Inform employees of what has happened, how it happened, and how it affects the firm.
- As a solo, it's not just you who is affected. It can also be your clients.
- If your data is compromised, consult the State Bar Ethics Line for guidance on how to proceed ethically and legally.

6) Recover

A. UNDERSTAND:

- Know who besides yourself has recovery responsibilities. Is it you alone? Did you get the cybersecurity insurance? What are they covering? Is it a third party?

B. ASSESS:

- Document every detail of the incident, including the response, recovery actions taken, and lessons learned, as you would prepare a trial notebook. Just like in a trial, if something happens to you, another attorney should be able to pick up your trial notebook and go to trial the same day, without skipping a beat.
- Before restoring data from a backup, confirm the integrity of the files. Ensure the issue is fully resolved to avoid compromising the backup.

C. PRIORITIZE:

- Do not try to do all the things all at the same time.
- As solos and attorneys, we are good at making lists. So, make one of everything that needs to be done. Then prioritize it based on the low, medium, and high impact categories. Develop a follow-up plan to address unresolved issues over time.

D. COMMUNICATE:

- Keep the report in a place where you can easily access it if you need to; hopefully, it never comes down to it. Print a copy, not just an electronic one.
- When setting goals for the following year, review the report. Refine your cybersecurity processes. Think about what improvements you can make. Implement them.

By adopting the NIST framework, solo attorneys can protect their and their client's sensitive information, prepare for cybersecurity threats, and establish a secure foundation for their practice. If there is one thing you take from this article, let it be this:

have a plan in place; if you don't know where to start, ask for help.

Cybersecurity is too important to leave to chance.

ABOUT THE AUTHOR:

Fatima Naeem is the founding attorney of Naeem Law Firm, PLLC, where she focuses on cyber law, data privacy, healthcare compliance, mediations, arbitrations, and guardianships. With a commitment to staying at the forefront of legal developments, she earned her LLM in Cyber Law and Data Privacy from Drexel University in 2023 and became Certified in Healthcare Compliance in 2024. Since graduating from Texas Tech University School of Law in 2015, she has dedicated herself to serving the community, starting with Lone Star Legal Aid before hanging her own shingle in 2019. Starting in June 2021, Fatima has served as the Chief Compliance Officer for HealthPoint, a Federally Qualified Health Center, and also as its General Counsel from 2023-2024. Find more about Naeem Law Firm at www.naeemlawfirm.com.

Transfers of Sensitive Personal Data to China (Including Hong Kong and Macau), Cuba, Iran, North Korea, Russia and Venezuela

Lori Bellows

How to assess whether a business needs to consider Executive Order 14117 Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern

In today's digital world where data is considered "free money," businesses are increasingly selling or transferring personal data to other countries.

Executive Order 14117, however, restricts transfer of Americans' bulk sensitive personal data (and US government-related data) when such access would pose an unacceptable risk to the national security of the United States. The Department of Justice has released its Final Rule that becomes effective on April 8, 2025.[1] Businesses should conduct a basic screening to identify the potential applicability of Executive Order 14117 and further understand its basic provisions.

1) Screening for Potentially Prohibited Transactions

If a business answers "yes" to both of the following questions, consider seeking advice from a regulatory specialist:

1. Will data be transferred to China, including Hong Kong or Macau, Cuba, Iran, North Korea, Russia or Venezuela?

These are the countries currently identified as countries of concern under the Final Rule.

2. Does the amount of data transferred rise to the following levels over the prior twelve months?

It is important to note that the thresholds below include data that has been anonymized, pseudonymized, de-identified or encrypted.

Geolocation data of 1,000 US persons or devices: includes data that identifies the physical location of an individual or device within 1,000 meters and includes GPS coordinates.

Biometric identifiers of 1,000 US persons: includes measurable physical characteristics or behaviors used to recognize or verify the identity of an individual such as facial images, voice prints and patterns, retina and iris scans, palm prints and fingerprints.

Human genomic data of 100 US persons or human 'omic data of 1,000 US persons: human 'omic data includes epigenomic, proteomic or transcriptomic data. If you aren't familiar with these data types, ask whether the data involves genetic material such as DNA, proteins in a biological system, RNA transcripts or anything similar as a general screening question.

Personal health data of 10,000 US persons: includes information that indicates, reveals, or describes the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare such as height and weight, vital signs, symptoms, test results, diagnostic or treatment, exercise habits and data on purchase or use of medications.

Personal financial data of 10,000 U.S. persons: includes information about an individual's credit, charge, or debit card or bank account, including purchases and payment history; and data in a bank, credit or other financial

[1] Certain affirmative due diligence and audit requirements will be phased in with an effective date of October 6, 2025. An explanatory fact sheet is provided by the DOJ.

statement, including assets, liabilities, debts or trades in a securities portfolio.

Personal identifiers of 100,000 persons: includes names linked to social security numbers, names linked to email addresses and IP addresses, government identification numbers and names linked to device identifiers.

Government-related data: includes ANY (1) precise geolocation data within geographic areas listed on the Department's public Government-Related Location Data List and (2) sensitive personal data marketed as linked or linkable to current or recent former employees or contractors, or former senior officials of the U.S. government.

2) The Executive Order and Rule that Businesses in Summary

Prohibited transactions include data brokerage and covered data transactions involving access to bulk human 'omic data or human biospecimens from which such data can be derived.

Data brokerage generally refers to the sale of, licensing of access to, or transfer of data where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.

Restricted transactions include vendor, employment, and non-passive investment agreements. These may be allowed if they comply with certain security requirements developed by the Department of Homeland Security's Cybersecurity and Infrastructure Agency.

U.S. persons engaged in **data brokerage with any foreign person** that is not a covered person[2] must contractually limit the foreign person from reselling or providing access to the data to a country of concern or covered person through a subsequent covered data transaction, among other requirements.

Circumvention rules prohibit US persons from knowingly directing any covered data transaction that is prohibited if conducted by a US person and from other actions designed to evade the regulations.

Exceptions are included for a variety of transactions such as certain corporate group transactions between a U.S. person and its foreign subsidiary or affiliate, if they are ordinarily incident to and part of routine administrative or business operations, such as human resources, payroll, taxes, permits, compliance, risk management, travel, and customer support.

U.S. companies are expected to develop and implement **compliance programs** based on their individualized risk profiles. Risk-based compliance programs may vary depending on a range of factors such as the company's size and sophistication, products and services, customers and counterparties, and geographic locations.

ABOUT THE AUTHOR:

Lori Bellows, JD, CIPP/EU/US, CIPM, FIPP, is a global technology lawyer specializing in practical operational guidance on international data and technology transactions.She currently serves as the Chief Privacy Officer and Chief Counsel for Global Data for the Solera companies headquartered in Texas. Solera provides high-tech solutions for the automotive and insurance industries in more than 90 countries.

[2] A "covered person" includes (1) foreign entities that are 50% or more owned by governments of the country of concern, organized under the laws of a country of concern, or have their principal place of business in a country of concern; (2) foreign entities that are 50% or more owned by a covered person; (3) foreign employees or contractors of countries of concern or entities that are covered persons; (4) foreign individuals primarily resident in countries of concern; and (5) persons designated as covered persons by the Department of Justice.

IN THE NEWS

by Maria Moffat

2025 TX 89(R) H.B. 1709

A new bill, sponsored by Rep. Giovanni Capriglione, is being introduced in this current session of the Texas Legislature. It relates to the regulation and reporting on the use of artificial intelligence systems by certain business entities and state agencies. This bill will also provide for civil penalties for violation. In section 1 of this Act, the title of the Act is the Texas Responsible Artificial Intelligence Governance Act. It would be included in Title 11 of the Texas Business & Commerce Code.

The act would require a deployer or developer that deploys, offers, sells, leases, licenses, gives, or otherwise makes available a high-risk artificial intelligence system that is intended to interact with consumer shall disclose to each consumer, before or at the time of interaction:

1. That the consumer is interacting with an artificial intelligence system;
2. The purpose of the system;
3. That the system may or will make a consequential decision affecting the consumer;
4. The nature of any consequential decision in which the system is or may be a substantial factor;
5. The factors to be used in making any consequential decision;
6. Contact information of the deployer;
7. A description of – (a) any human components of the system; (b) any automated components of the system; and (c) how human and automated components are used to inform a consequential decision; and
8. A declaration of the consumer's rights under this section.

The Act also calls for the creation of the Texas Artificial Intelligence Counsel to monitor
these provisions, along with training and research for state agencies and local governments on the ethical use of artificial intelligence systems.

AI Summit in Paris, France Took Place This Week

The third annual Artificial Intelligence (AI) Summit took place for two days in Paris, France. The summit was opened by French President Emmanuel Macron. It was attended by global political and business leaders including US vice-president, JD Vance, the Indian prime minister, Narendra Modi, the Canadian PM, Justin Trudeau, and the head of the European Commission, Ursula von der Leyen. Leaders from more than 100 countries attended in an effort to discuss how to reach a consensus on guiding the development of AI.

The Summit had several emerging highlights:

1. The world's leaders still have disagreements and tensions on the rising emerging technology of AI and how and to what extent it should be regulated.
2. Both the United States and United Kingdom declined to sign the Artificial Intelligence Action Summit declaration on "inclusive and sustainable" AI published at the end of the summit. The declaration called for policies to achieve inclusive, transparent and safe protocols for governing and regulating AI. During this summit, differences started to arise between countries as to how much regulation of AI should be enacted vs how much should AI be allowed to grow to promote a county's productivity, innovation and development.
3. The consensus of the main area of discussion and concern among leaders differed more this year than in the prior two years. Safety did not rise to the top of concerns as it did at the UK Summit in 2023. The UK Prime Minister also contended that the diplomatic declaration did not go far enough on topics including the technology's impact on national security of a country. Concerns were raised by Macron about the trajectory of AI as "unsustainable." The General Secretary of the UNI Global Union also stated an "engine of inequality" might be created by driving productivity gains at the cost of workers' welfare.

The recent product launched by ChatGPT is one example of how AI will impact the labor market in the next two to three years. The percentage of workers' jobs that are overtaken by AI will increase much more than expected globally.

ChatGPT Launches new product "Deep Research"

ChapGPT launched, earlier this month, a new product known as "Deep Research" and its features will enhance ChatGPT with the capabilities of a "research analyst" that automates time-consuming research by retrieving, analyzing, and synthesizing online information.

Unlike standard chatbot interactions, Deep Research operates independently for 5 to 30 minutes, browsing the web, interpreting content, and compiling structured reports with citations, the company said. Powered by a specialized version of OpenAI's upcoming o3 model, it's optimized for reasoning and data analysis.

Recent Actions by the Federal Trade Commission (FTC)

Bureau of Consumer Protection: Technology, Privacy and Security

The FTC finalized an order against IntelliVision Technologies Corp. prohibiting the company from misrepresenting the accuracy and efficacy of its AI-powered facial recognition software, comparative performance of the technology, and its ability to detect spoofing.

The order further requires the company to have competent and reliable testing before making any further representations about its technology. The company has to document such testing as well, to include dates and results of the tests; methodology of the tests, course and number of images used, any techniques to modify images; extent of different people used in the images; demographic information collect on the images and information about how the images regarding skin tone are collected used in testing. This order settles allegations that the company made false and misleading claims that its facial recognition software was free from bias based on gender or race.

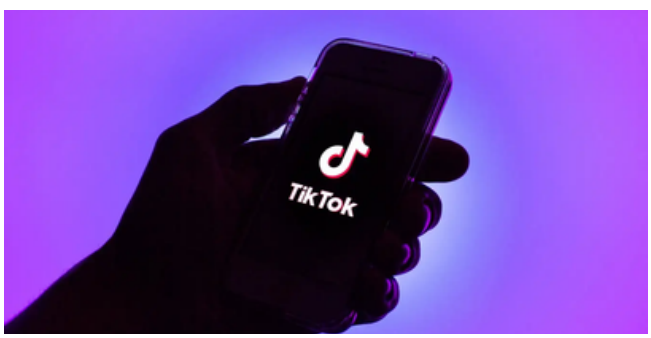
Jury Returns Verdict for Claims of Violation of Texas Penal Code by E-Discovery Vendor

On November 6, 2024, a jury returned a verdict in favor of Plaintiff Angelyn A. Olson in a Tarrant County lawsuit where she alleged that she was involved in other litigation during which e-discovery service provider (Consilio) (Defendant The Consilio, LLC) was engaged to collect her personal emails. In that other litigation, Plaintiff Olson had agreed to a collection of her emails from her personal email account that were responsive to certain search terms. Plaintiff argued to the jury that her lawyer had emphasized the search terms applied to her email collection should be applied at the point of collection, rather than after a full collection of her email account. Instead, Plaintiff argued that Consilio downloaded all of her emails (34,000 files) and then applied the search terms.

She further alleged that she had sensitive information in her emails (i.e. medical information, attorney client privileged information and other private information). Plaintiff Olson asserted claims against Consilio and its representative for invasion of privacy and harmful access by a computer in violation of Texas Penal Code Title 7, Section 33.02(a) (which states - if a person "knowingly accesses a computer, computer network, or computer system without the effective consent of the owner," they commit an offense under the code). Plaintiff further asserted a cause of action under Tex. Civ. Prac. & Rem. § 143.002 and a negligence per se claim that relate to the alleged violation of the Texas Penal Code Title 7, Section 33.02(a) and therefore allowed her to recover civil damages. The jury found The Consilio, LLC committed such violation and awarded Plaintiff damages as a result.

Law Banning Tik Tok on Hold and Tik Tok is now Available for iPhones and Android

TikTok is now available again in the App Store for iPhones and other Apple devices as well as the Google Play Store for Android phones and tablets. President Donald Trump signed an executive order on January 20, 2025, that directed the Department of Justice not to enforce the ban on TikTok for 75 days. Apple and Google Play had previously not allowed the TikTok in their stores for download due to the law banning TikTok in the US.



However, recently US Attorney General Pam Bondi has sent a letter to Apple assuring that Apple won't be fined for hosting the app, according to Bloomberg.

Texas AG Sues Allstate for Violations of Texas Privacy Law in First Enforcement Action under Texas Data Privacy and Security Act

On January 13, 2025, Texas Attorney General Ken Paxton announced that the Texas Attorney General's office has filed several lawsuits against Allstate and its subsidiary, Arity (together, "Allstate"), for the unlawful collection, use and sale of precise geolocation data collected through Allstate's mobile apps, in violation of Texas Data Privacy and Security Act (which requires notice regarding how a company uses consumers' sensitive data including geolocation data).

According to the Attorney General, Allstate used its subsidiary Arity to pay third-party developers to embed software into various mobile apps, including GasBuddy, Fuel Rewards and Routely. The software allowed Allstate to track consumers' location and movement in real time and to build up a database of consumer driving behavior. The Attorney General has alleged that Allstate collected information on over 45 million consumers nationwide and then when a consumer requested a quote for insurance, the lawsuits allege that Allstate and other insurers would use that consumer's data to justify increasing their car insurance premium or to drop them from coverage.

ABOUT THE AUTHOR:

Maria Moffatt

Maria Moffatt is Partner at Gerstle Snelson, LP and practices in the areas of construction and employment/labor. She is Board Certified in Construction Law. Received her J.D. from Southern Methodist University. She is member of the State Bar of Texas and is council member to the State Bar of Texas Computer & Technology Section, 2023-2026.

The State Bar of Texas International Law Section
and the Computer & Technology Section Present

NAVIGATING THE FUTURE OF AI: LATEST DEVELOPMENTS IN AI REGULATION

Free Webinar
1 Hour CLE Credit

MARCH 21, 2025
12:00 - 1:00 pm CST

Panelists:

Lindsay J. Forbes, Counsel, Global Trade Compliance, Lenovo US

Clarissa Benavides, Toyota Financial Services, Managing Counsel – Privacy, Artificial Intelligence & Cybersecurity

Lavonne Burke, Vice President - Security, Resiliency, IT & AI Legal, Dell Technologies

REGISTER NOW

This webinar is being presented jointly by the International Law Section and the Computer & Technology Section and will be available for replay on the ILS website at ilstexas.org.

INTERNATIONAL LAW SECTION
THE STATE BAR OF TEXAS
1975-2025
CELEBRATING 50 YEARS

COMPUTER AND TECHNOLOGY SECTION

Visit our websites:**ilstexas.org | sbot.org**