POLSINELLI | What a law firm *should* be.™

Technology Transactions & Data Privacy

2025 REPORT

It is hard to believe that we are starting the 25th year of the 21st century. The rapid evolution that technology, privacy and data security have undergone these last 25 years is mind-bending. Yet, as we enter 2025, it still feels like we are at the beginning of "the future."

Our fifth annual Technology Transactions & Data Privacy Report explores critical trends in technology deals, privacy frameworks and data protection. This year, we highlight regulatory developments, litigation risks and best practices for safeguarding sensitive information.

Online tracking litigation is surging, with claims under the California Invasion of Privacy Act (CIPA), Video Privacy Protection Act (VPPA) and Federal Wiretap Act (FWA) prompting businesses to reassess privacy policies and consent mechanisms on their websites as well as the processes through which they vet and deploy tracking technologies. Artificial intelligence adoption continues to reshape entire industries, compelling general counsels to continually balance innovation with risk.

In 2024, seven new states passed consumer privacy laws, expanding data protection requirements and complicating compliance efforts. Data breach notification laws also continue to tighten, reinforcing the importance of cybersecurity investments. Safe harbor provisions in Ohio and Tennessee offer protections to companies that meet emerging frameworks, reflecting a growing legislative focus on incentivizing stronger security practices. This is further accentuated by the EU's NIS2 directive and CISA's drive to expand U.S. security frameworks for critical infrastructure through stricter incident reporting and supply chain security requirements.

Our report also focuses on the evolving landscape of Software-as-a-Service (SaaS) agreements. As SaaS adoption grows, negotiations around data privacy, vendor liability and contract terms are increasingly complex given that many of the issues outlined above must be accounted for in SaaS transactions most often on a bespoke transaction-by-transaction basis.

Finally, we foresee that regulatory shifts may very well redefine the digital asset landscape. We anticipate that Web3 and digital assets will continue to grow significantly, with stablecoins and blockchain technologies gaining renewed traction in 2025.

In this report, Polsinelli lawyers provide thoughtful information and analysis at the intersection of innovation and compliance, giving actionable insights for legal professionals, technology leaders and policymakers.

Polsinelli remains committed to guiding clients through these transformative times that lie ahead.

Greg M. Kratofil, Jr.
Technology Transactions
& Data Privacy Chair

Contents

Pixel-Tracking, the VPPA and the Problem with Class Certification

Mark A. Olthoff
Shareholder
Kansas City

Courtney P. Klaus
Associate
Kansas City

As technology evolves, old laws can gain new life. Over the past few years, plaintiffs have been using decades-old privacy statutes, including pen register, wiretapping, interception and video protection statutes, taking what were previously considered well-established rules with a relatively limited scope and using them to challenge businesses that incorporate popular new technologies to engage with their consumers. Typically, these lawsuits have not progressed very far — most either result in a settlement or are dismissed. But a recent decision reflects what might happen when these cases proceed past the pleading stage.

In one of the first cases of its kind to reach a class certification determination, the United States District Court for the Southern District of Florida recently refused to certify a proposed class of Univision NOW subscribers who alleged that Univision NOW shared their identities and viewing histories with Meta Platforms. Specifically, the class representatives alleged Univision NOW, a Spanish-language video-streaming service, used a tracking pixel — Meta Pixel — to collect and transmit their personal viewing information without their knowledge and consent in violation of the federal Video Privacy Protection Act (VPPA).

The plaintiffs asserted that Univision NOW embedded a Meta Pixel on its website to track users as they navigated the site, and the pixel then reported back to the pixel's owner, Meta Platforms. The plaintiffs sought class certification of all Univision NOW subscribers whose information was allegedly disclosed to Meta.

History of the VPPA

Congress passed the VPPA in 1988 in response to concerns about the privacy of consumers' video rental history, particularly after Supreme Court nominee Robert Bork had his video rental history exposed in a newspaper article during his confirmation hearing. In short, the VPPA prohibits "video tape service providers" from knowingly disclosing a consumer's personal identifying information together with their video viewing history without informed written consent. It provides actual or liquidated damages of $2,500 per violation, plus attorney's fees, litigation costs and injunctive relief. The VPPA, historically applied to video store rentals, has seen a recent increase in use in privacy class actions against website owners with video functionality on their websites. Plaintiffs in these more recent lawsuits contend that a tracking pixel — such as a Google pixel or a Meta Pixel — embedded on a website constitutes an unlawful disclosure of their video viewing history.

The perceived strength of these claims has fluctuated significantly over the past two years. By fall 2023, it was thought that the VPPA class action wave would be slowed by a relatively high dismissal rate. While over 100 VPPA class actions were brought against online news outlets, streaming services, retailers and others that integrated pixel tracking,

CONTINUED ON PAGE 3

CONTINUED FROM PAGE 2

17 were dismissed by courts, 29 were voluntarily dismissed by plaintiffs and only 19 resulted in classwide settlements or other public statements. However, a Second Circuit Court of Appeals opinion from earlier this year revived a previously dismissed VPPA claim, purportedly breathing some new life into the viability of these claims. The Southern District of Florida, however, is one of the first courts to consider the certification of a VPPA class.

The Univision NOW Case

In spring 2023, subscribers to Univision NOW brought a claim against the streaming service under the VPPA for its use of the Meta Pixel. Although Univision NOW filed a motion to dismiss, the district court denied the motion. The court was unpersuaded by Univision NOW's arguments that the allegations against it were too vague, that it did not act "knowingly" and that the plaintiffs lacked standing. The case was allowed to proceed, and the plaintiffs had seven months to gather enough evidence to certify their class.

After class certification discovery, the plaintiffs filed their certification motion seeking to represent a class of Univision NOW subscribers. On October 1, 2024, nearly one year after rejecting Univision NOW's motion to dismiss, the district court rejected the plaintiffs' request for class certification, largely due to their failure to satisfy "numerosity," one of the four essential elements required for class certification under the Federal Rule of Civil Procedure 23(a). The plaintiffs were unable to prove the numerosity requirement because the evidence was too speculative to rely on to identify a sufficiently large number of individuals reportedly affected by Univision NOW's VPPA violation. The plaintiffs had argued that Univision NOW disclosed the viewing information of over 35,000 subscribers but acknowledged there were a number of impediments to Univision's transmission of information to Meta. The plaintiffs' theory of automatic data transmission was undercut by their concessions to Univision NOW's expert testimony that various conditions must be met for the pixel to automatically transmit. In addition to viewing or selecting a prerecorded video through the website, a subscriber must also have (1) a Facebook account at the time video was selected, (2) used a web browser that did not block the pixel by default, (3) been simultaneously logged into the subscriber's own Facebook account while selecting the video, (4) been simultaneously logged into Facebook on the same device that the subscriber used to select the video, (5) been simultaneously logged into Facebook using the same browser from which the subscriber selected the video and (6) not deployed any number of browser settings or add-on software that would have blocked the pixel. While the court found that the putative class members were ascertainable because the number of subscribers could be identified with reasonable feasibility, class certification was not warranted because the plaintiffs failed to show that Univision NOW disclosed the personal information and record of videos viewed by a single subscriber (including the three named plaintiffs). The court referred to the plaintiffs' failure to supply anything more than speculation of the class size as "particularly problematic."

The plaintiffs tried to save their class certification request by reducing the potential class to approximately 17,000 individuals, based on estimates of individuals who used Facebook and certain web browsers, but the court found that plaintiffs had ignored certain expert testimony that limited this number to roughly 15,000. The court then concluded that even those estimates were still too speculative based on the conditions required for transmission of the information. Without the ability to determine class size, the plaintiffs failed to satisfy the numerosity requirement. With the plaintiffs having failed to establish this essential requirement, the court declined to evaluate whether the class would have satisfied any of Rule 23(a)'s other elements, namely, commonality (whether the class would have shared legal questions among the group), typicality (whether the representative plaintiffs' claims were typical of the class) or adequacy of representation.

The U.S. District Court for the Southern District of Florida's focus on numerosity reflects that plaintiffs have a substantial burden to prove with evidence that they can identify a class of people who were affected by the claims alleged. The burden is on the plaintiff to prove their claims for certification, not on the defendants to prove the negative. Compared to commonality or typicality, which usually require a deeper examination of the legal issues and factual similarities across the class, numerosity usually only requires basic evidence of class size. While numerosity is often an overlooked element in class actions, the Univision NOW case is an example where the courts will not simply give lip service to an allegation that the number of people impacted is significant; instead, plaintiffs must bring forth proof that the number of individuals affected by the conduct meets class certification requirements. Given that pixel-tracking allegations may rely on a set of assumptions regarding who has accessed a website, what they have accessed, when they did so and how, as well as what conditions exist for the transmission of data, defendants may be able to stop VPPA classes from being certified, reduce litigation costs and avoid expensive payouts.

Developments in Online Tracking Litigation: Risks Hiding in Plain Sight on Your Site

Starr Turner Drum
Shareholder
Los Angeles

Xeris E. Gregory
Associate
Birmingham

Jonathan E. Schmalfeld
Associate
St. Louis

Litigation involving online tracking experienced a substantial year-over-year increase from 2023 to 2024, with a particularly significant increase in cases asserting claims under the California Invasion of Privacy Act (CIPA). Other web tracking-based claims also saw significant increases in 2024, including claims alleging violations of the Federal Wiretap Act (FWA) and claims asserting violations of other states' multiparty consent wiretapping statutes. While Video Privacy Protection Act (VPPA) claims experienced a slight decline during the first part of the year, filings started to creep up again after the Second Circuit's decision in *Salazar v. NBA*, No. 23-1147 (2d Cir. Oct. 15, 2024), held that a broad scope of individuals who may not have purchased video services could still be considered "consumers" under the VPPA. The plaintiffs' bar also advanced new claims against several e-commerce companies alleging online tracking-based violations of the Song-Beverly Credit Card Act of 1971. All of the foregoing causes of action have strict liability statutory penalties ranging from $250 to $10,000 per violation, which can become a significantly expensive problem even with relatively little website traffic.

The increase in online tracking lawsuits reflects a rapidly evolving legal landscape, with web tracking class actions becoming a persistent challenge for businesses across industries.

Tracking Technologies That Create Litigation Risk

There are numerous names for online tracking technologies: pixels, beacons, tags, cookies, scripts, etc. The functionalities can vary, but, at bottom, the tracking technologies that create litigation exposure are bits of code that collect and then share data about user interactions on a website. Third-party social media platforms like Meta, TikTok, LinkedIn, etc. often develop these code components so that businesses can leverage marketing opportunities on their platforms. Trackers can be configured to capture information such as operating system, browser type, IP address, time and device details, and more specific information, including how long a person spends on a web page, which buttons a person clicks, which pages a person viewed and which search terms a person entered. The code for these technologies can be viewed by anyone who visits the website on which they are deployed with a few mouse clicks, and some social media platforms permit users to find information about which organizations have leveraged these trackers to share that user's information with that social media platform.

Online Tracking Litigation Background

This surge in online tracking litigation has not come from legislatures passing new laws. Instead, the plaintiffs' bar has been testing the bounds of the application of old laws passed in the 1960s through the 1980s on new technology.

For example, CIPA was passed in 1967 and prohibits "wiretapping" and the use of a "pen register" or "trap and trace device" without the consent of the parties to a communication. The FWA was passed in 1968 and updated in relevant part in 1986. It prohibits intercepting a communication by a nonparty to the communication without consent of one party to the communication, and even if one party does consent to the interception, the interception may not be conducted for a criminal or tortious purpose. The VPPA was passed in 1988 and prohibits "video tape service providers" from disclosing video rental information without a consumer's consent.

The unifying theory when alleging that new technologies are violating these old laws is that tracking technologies allegedly disclose private information to third parties without consent. Outside of a recent ruling by the Massachusetts Supreme Court in *Vita v. New England Baptist Hospital*, SJC-13542 (Mass. Oct. 24, 2024), holding that its wiretapping law did not extend to online tracking technology, courts largely have not rejected these theories outright. In some cases, claims have been brought against websites that use cookie banners that ostensibly present users with an option to opt out but allegedly either transmit information before the user can

CONTINUED ON PAGE 5

CONTINUED FROM PAGE 4

opt out or continue to transmit information to third parties despite the user's selection to opt out. Defending these claims requires an analysis of the underlying technology on the website, the relevant disclosures made to users and any terms to which users are bound.

A Special Note for Health Care Defendants

Although no industry is safe from these claims, health care providers have been consistent targets in web tracking litigation during the past few years. The uptick correlated with a **U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) bulletin** issued in December 2022. The HHS OCR Bulletin asserted that information collected on a covered entity's website could constitute protected health information (PHI), even if an individual did not have an existing relationship with the covered entity and even if the information collected did not include specific treatment or billing information. Multiple lawsuits have been filed by website visitor plaintiffs against health care providers that had website analytics technologies installed on sections of their websites, particularly in the context of alleging that tracking on covered-entity websites violates the "criminal or tortious" provision of the FWA by allegedly constituting a HIPAA violation.

In November 2023, the American Hospital Association, the Texas Hospital Association and two health care providers filed a lawsuit to enjoin enforcement of the HHS OCR Bulletin. On June 20, 2024, the court vacated a portion of the HHS OCR Bulletin in a win for HIPAA-covered entities.[1] The court found the HHS OCR Bulletin required "covered entities to perform the impossible" and concluded that an individual's IP address combined with a visit to a web page addressing specific conditions or health care providers is not individually identifiable health information under HIPAA. While this may have lessened the threat of regulatory enforcement tied to this particular type of tracking, the plaintiffs' bar has thus far not retreated from asserting covered entities' website tracking activities constitute an FWA violation.

Avoiding Website Tracking Litigation Risk

The simplest way for companies to avoid website tracking litigation risk is to not deploy any third-party tracking tools on their web properties. This blunt approach could have negative business impacts, though, and a more nuanced approach can simultaneously preserve marketing benefits and reduce litigation risk. To take a more tailored approach to mitigating risk, companies can:

- Use internal resources or outside counsel to assess which third-party tracking technologies are used on the company's web properties.
- Work with web development and marketing teams to pressure test the utility of third-party trackers for the business and determine if any should be removed or should be isolated to specific pages or sections of the company's website.
- Consider the implementation of a consent management platform and implement geofencing and use case-specific opt-in configurations on those platforms.
- Assess and update website privacy policies to ensure they accurately disclose the use of tracking technologies.
- Assess and update terms of use to ensure the company is satisfied with its choice of forum and dispute resolution process.
- Consider opportunities to bind users to the company's terms of use through clickwrap or similar mechanisms and implement same.
- Monitor and regularly audit all of the foregoing.

[1] *American Hospital Assn. v. Becerra,* No. 4:23-cv-01110-P, (N.D. Tex. June 20, 2024).

Rule of Lenity as a Shield Against Statutory Damages: Massachusetts Supreme Judicial Court Takes a Fresh Look at 1970s Era Wiretap Statutes

John C. Cleary
Shareholder
New York

Shundra Crumpton Manning
Associate
Nashville

Tyler G. Anders
Associate
Nashville

Since 2022, plaintiffs have filed a tsunami of class action lawsuits alleging violations of state and federal wiretap statutes based on the use of tracking technologies such as pixels and session replay tools. Plaintiffs and their counsel, often veterans of the data breach class action wars, see nothing but upside in this novel avenue of attack on often settled e-commerce technologies and market practices. First, the statutes themselves call for statutory damage awards, regardless of injury and often regardless of fault or even causation. Second, drawing on the considerable creativity of the plaintiffs' class action bar, these new cases have creatively resurrected and repurposed decades-old wiretap statutes that were originally enacted to curtail eavesdropping on telephone lines and various other trap and trace tactics. These vestiges of the Warren Court era and the resulting outcry over questionable police and law enforcement tactics are today enjoying a "second wind" as instruments of novel and expensive civil litigation directed at technologies and problems that never even existed when the laws were passed.

These suits have sparked concern in companies that use tracking technologies on their website to share data with third parties, such as Google, Meta or TikTok. In these lawsuits, plaintiffs typically argue that the federal and state wiretap statutes encompass the improper tracking of a user's interactions on a website without notice and consent. While the federal and state wiretap statutes originally only applied to telephones and person-to-person messages communicated through the use of wire or cables, with the advent of the internet, these statutes have now been amended to include electronic communications but still fall far short of comprehensive, intelligible and evenhanded regulation of privacy in the e-commerce sphere.

Deepening the problem, courts have varied, sometimes dramatically, on whether wiretap statutes can serve as the proper mechanism by which to hold companies accountable for tracking customer interactions and data without notice and consent. This volatility, particularly at the pleading stage, has impaired the ability of law-abiding companies to get their arms around this subject matter area and discern what the law permits and prohibits in the present day, on pain of high levels of potential exposure to statutory damages.

For example, courts in California have grappled with the scope and meaning of "trap and trace" devices under the state's wiretap statute.[1] Some courts have focused on the "expansive language" of the "California Legislature's chosen definition" of such devices to allow claims alleging that website tracking technologies amount to an unlawful "pen register" or a trap and trace device to proceed past the pleading stage.[2] Other courts have taken a broader approach, denying such claims on public policy grounds.[3] The result has been inconsistent rulings on when an organization might be liable for its use of website tracking technologies.

The Rule of Lenity

But all is not lost. A recent decision by the Massachusetts Supreme Judicial Court (SJC) — *Vita v. New England Baptist Hosp.*, No. SJC-13542, 243 N.E.3d 1185 (2024) — could provide hope to courts, companies and their defense counsel looking for a better framework. The Massachusetts SJC, recognizing the ambiguity in wiretap statutes and acknowledging that such statutes have both criminal and civil application, applied the rule of lenity.

The rule of lenity, also known as the rule of strict construction, is a principle typically used in the context of criminal law, stating that when a law is unclear or ambiguous, the court should apply it in the way that is most favorable to the defendant. When a statute has both civil and criminal applications, such as wiretap statutes, courts have held that the rule of lenity may apply.

[1] California Invasion of Privacy Act (CIPA), Cal. Pen. Code § 638.51.
[2] *See Greenley v. Kochava*: 684 F. Supp. 3d 1024 (S.D. Cal. 2023).
[3] *See Licea v. Hickory Farms LLC*, No. 23STCV26148, 2024 WL 1698147 (Cal. Super. Mar. 13, 2024).

CONTINUED ON PAGE 7

CONTINUED FROM PAGE 6

In *Vita*, the plaintiff alleged that two hospitals violated the Massachusetts Wiretap Act by collecting and transmitting her browsing activities on the hospitals' websites. The plaintiff argued that the collection of her interactions with the websites fell within the meaning of the "interception" of "wire communication" protected by the Wiretap Act. The Massachusetts SJC held, "[b]ased on our review of the text of the Wiretap Act and its legislative history, we cannot conclude with any confidence that the Legislature intended 'communication' to extend so broadly as to criminalize the interception of web browsing and other such interactions."[4] The court held that the statute, including amendments thereto, was meant to "prohibit new and evolving technological means of secret electronic eavesdropping on such person-to-person conversations or messaging."[5] The court found that the plaintiff's allegations did not claim the interception of person-to-person conversations or messaging of the kind clearly within the Wiretap Act's ambit. As stated by the court, "[b]rowsing and accessing the information published on a website is significantly different from having a conversation or sending a message to another person. . . . The user is also not engaging in a conversation but accessing published information and databases."[6] The court also held that Massachusetts case law has never extended the meaning of "communication" beyond person-to-person interactions. After reviewing the text of the statute, legislative history and case law, the Massachusetts SJC concluded that the statute was ambiguous. Since the statute was ambiguous, the court held that the rule of lenity applied (i.e., defendants were entitled to the benefit of any rational doubt). On this basis, the court dismissed *Vita's* claims against the hospitals.

While the ruling in *Vita* is promising, some federal courts, when evaluating claims under CIPA and the Pennsylvania Wiretapping and Electronic Surveillance Control Act, have rejected the reasoning set forth in *Vita*, instead finding that there are "no ambiguities, let alone grievous ones, in the statutes," and engaging in a "hyper-technical reading of the statute[s]" is inconsistent with the purpose of the statutes.[7]

What To Expect in 2025

Moving forward, we can expect defendants to use creative defenses to wiretap claims, such as the rule of lenity. We also anticipate a renewed focus on legislative history. For example, the California legislature enacted Assembly Bill (AB) 929 in 2015 to create a comprehensive framework governing the use of pen registers and trap and trace devices.[8] Before 2015, California had not enacted a specific statute regulating California law enforcement's use of pen registers and trap and trace devices. Even a cursory review of the AB 929 legislative history makes clear the amended law was intended to address this narrow issue and was never intended to regulate website tracking technology.[9]

Final Thoughts

While some defendants have achieved success in defeating claims for violation of wiretap acts in the web tracking context, there are still cases being regularly brought by plaintiffs. Companies should expect these lawsuits to continue, as more legal principles are being used to prosecute and defend these lawsuits. Companies that would like to continue to use web tracking tools on their websites should provide notice of the use of such technologies and obtain express consent from users.

---

[4] *Vita*, 243 N.E.3d at 1188.
[5] *Id.*
[6] *Id.* at 1199.
[7] *Howard v. Lab'y Corp. of Am.*, No. 1:23-CV-00758, 2024 WL 4250677, at *8 (M.D.N.C. Aug. 8, 2024), report and recommendation adopted, No. 1:23-CV-758, 2024 WL 4326898 (M.D.N.C. Sept. 27, 2024); James v. Walt Disney Co., 701 F. Supp. 3d 942, 960 (N.D. Cal. 2023), motion to certify appeal denied, No. 23CV02500EMCEMC, 2024 WL 664811 (N.D. Cal. Feb. 16, 2024).
[8] Cal. Penal Code § 638.50-55.
[9] *See* Pen Registers: Authorized Use: Hearing on AB 929 Before the Assembly Comm. on Priv. and Consumer Protection, 2015-2016 Sess. 5 (Ca. 2015); Pen Registers: Authorized Use: Hearing on AB 929 Before the S. Public Safety Comm., 2015-2016 Sess. 1 (Ca. 2015).

Examining Cybersecurity Critical Infrastructure Regulations in the U.S. and EU

Sarah S. Glover
Shareholder
Birmingham

Greg J. Leighton
Privacy & Incident Response Vice Chair
Chicago

Romaine C. Marshall
Shareholder
Salt Lake City

Mary Ann H. Quinn
Associate
Birmingham

Business entities within the critical infrastructure sector provide essential products and services for the public, and disruptions to these entities' operations arising from a cyberattack can threaten national security and public safety. This reality was illuminated after the 2021 cyberattack on Colonial Pipeline. Last year, Tom Fanning, the chair of the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Advisory Committee, provided **a retrospective on this watershed moment in American history**, reflecting:

"On May 7, 2021, a ransomware attack on Colonial Pipeline captured headlines around the world with pictures of snaking lines of cars at gas stations across the eastern seaboard and panicked Americans filling bags with fuel, fearful of not being able to get to work or get their kids to school. This was the moment when the vulnerability of our highly connected society became a nationwide reality and a kitchen table issue."[1]

One need only peruse CISA's list of the types of companies that fall within the critical infrastructure sector – hospitals, food and agricultural businesses, banks – to appreciate what large-scale cyberattacks against those types of organizations could similarly mean for the American public. This is especially true in light of **warnings from the U.S. government about potential cyberattacks against critical infrastructure from nation-state actors out of China and Russia.**

Securing critical infrastructure is not a singularly American concern. As is typical when it comes to data security and privacy regulation, the European Union has led the way globally in terms of prophylactic regulations. While **the U.S. government has outwardly expressed alarm and focus on this topic**, it has not taken the same hands-on approach as its European counterparts. **The U.S. government has largely left the implementation of technical controls within critical infrastructure to industry group development and private participation.**

The policy challenges of regulating millions of primarily private-sector companies in the U.S. have enabled an amalgamation of overlapping and complex reporting requirements and a lack of prescriptive security controls to date.

Examining and contrasting the controlling critical infrastructure frameworks in the EU and U.S. might shed some light on where the U.S. could be headed if it decides to ramp up regulations in this space. And, for those U.S. companies that are operating in the EU, it is important to understand the developing critical infrastructure regulatory landscape that they may already be subject to abroad.

European Critical Infrastructure Security Framework

In 2006, the European Union issued the **Communication from the Commission on a European Programme for Critical Infrastructure Protection (EPCIP)**. At this time, policymakers and lawmakers were primarily focused on protecting critical infrastructure from terrorist attacks, so the EPCIP did not mention cybersecurity or set out any specific security controls. However, the EPCIP did set out a protection framework based on an "all-hazards" approach, which included:

- A procedure for identifying and designating entities providing critical infrastructure;
- An information-sharing process and plan, including a warning network and use of expert groups;
- Support for member states;
- Contingency planning.

The EPCIP framework became the backbone of the Network and Information Systems Directive (NIS1), signed in 2016. NIS1 was the EU's first piece of EU-wide legislation on cybersecurity, and it provided for legal measures to boost the overall level of cybersecurity in the EU, but with a focus on critical infrastructure. NIS1 established the NIS Cooperation Group, as well as a network of

CONTINUED ON PAGE 9

CONTINUED FROM PAGE 8

Computer Security Incident Response Teams to facilitate the exchange of information and the provision of support during actual incidents, respectively.

While NIS1 was being transposed to the laws of the EU's member states, the threat landscape continued to evolve into the cyber domain, and by 2019, EU officials noted a continuing lack of cyber resilience of businesses across critical infrastructure sectors. These concerns motivated EU lawmakers to further define and update the scope of the law to create a piece of legislation that had staying power to meet current risks and future challenges in a rapidly changing environment.

NIS2 is the recent product of this effort and is currently a hot topic across industries for organizations operating in the EU. Signed in 2022 and going into effect in January of 2025, **NIS2 is the most recent and most widely applicable critical infrastructure regulation in the EU**. It is less voluntary than NIS1, covers more industries and prescribes specific cybersecurity measures for critical infrastructure entities. NIS2 requires the EU member states to implement NIS2's requirements for both public and private entities. Specifically, NIS2 requires that member states ensure that covered entities take appropriate technical, operational and organizational measures that include:

- Policies on risk analysis and information system security;
- Incident handling;
- Business continuity, such as backup management and disaster recovery, and crisis management;
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- Basic cyber hygiene practices and cybersecurity training;
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- Human resources security, access control policies and asset management;
- The use of multifactor authentication or continuous authentication solutions; secured voice, video and text communications; and secured emergency communication systems within the entity, where appropriate.

While it does contemplate security measures for suppliers, NIS2 does not directly regulate them or define the scope of the affected supply chain. Entities that are preparing for NIS2 compliance may begin to flow down certain security requirements to their partners, such as the requirement to conduct risk assessments, establish incident reporting and vet security controls. So third parties and suppliers can expect to see NIS2 initiatives trickle down into their contracts with covered entities.

Other critical infrastructure security frameworks exist within the EU, such as the **Digital Operations Resilience Act (DORA)** proposal for the financial sector and the European Electronic Communications Code (EECC). These frameworks are meant to function together with NIS2 in the interest of maintaining a strong relationship and exchange of information between the sectors covered by NIS2. Where DORA, for example, provides for more

CONTINUED ON PAGE 10

CONTINUED FROM PAGE 9

stringent security requirements for financial companies, NIS2 is meant to establish a security baseline across all sectors.

U.S. Critical Infrastructure Security Framework

After 9/11, the Department of Homeland Security (DHS) was positioned to bring the core homeland security initiatives under more-unified leadership, but critical infrastructure regulation remains highly distributed throughout the federal government even today.

One of the foundational critical infrastructure policy documents marking the shift away from counter-terrorism security was the **2013 Presidential Policy Directive 21 (PPD-21)**, which placed less focus on the dangers of terrorism and more focus on an all-hazards approach. PPD-21 contains the most widely accepted definition of "critical infrastructure" as the systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

PPD-21 also named 16 critical infrastructure sectors, and **approximately 13 million business entities make up these sixteen sectors as of April 2024**.

As depicted below, DHS is one of several Sector Risk Management Agencies (SRMAs) responsible for critical infrastructure security regulation.

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

CHEMICAL — CISA	DAMS — CISA	FINANCIAL — Treasury	INFORMATION TECHNOLOGY — CISA
COMMERCIAL FACILITIES — CISA	DEFENSE INDUSTRIAL BASE — CISA	FOOD & AGRICULTURE — USDA & HHS	NUCLEAR REACTORS, MATERIALS & WASTE — CISA
COMMUNICATIONS — CISA	EMERGENCY SERVICES — CISA	GOVERNMENT FACILITIES — GSA & FPS	TRANSPORTATIONS SYSTEMS — TSA & USCG
CRITICAL MANUFACTURING — CISA	ENERGY — CISA	HEALTHCARE & PUBLIC HEALTH — HHS	WATER — EPA

In addition to these SRMAs, other agencies have issued industry-specific regulations regarding cybersecurity incident reporting for critical infrastructure entities, including the Federal Communications Commission, Nuclear Regulatory Commission and Securities and Exchange Commission.

In 2018, CISA was established as an operational component of DHS charged with **"mobilizing a collective defense to understand and manage risk to our critical infrastructure and associated National Critical Functions" as they relate to cyber and physical threats**. CISA is at the center of a new rulemaking effort to establish the implementing framework for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) (6 U.S.C. §§ 681-681g), enacted in March of 2022. CISA released a notice of proposed rulemaking on March 27, 2024, that requires in part that critical infrastructure companies report cybersecurity incidents within 72 hours. This reporting requirement is not a replacement for all of the other sector-specific incident reporting obligations described above. The final rule is expected sometime in 2025, with reporting requirements taking effect in 2026. While CISA seems to be poised to eventually be the home base for critical infrastructure security regulation, CIRCIA does not contain, in the statute or in the proposed rulemaking, a list of specific controls and requirements to elevate the security baseline for critical infrastructure companies in the U.S.

Additionally, CISA just released the proposed National Cyber Incident Response Plan (NCIRP), on December 16, 2024, for public review and comment. The NCIRP outlines a proposed framework for how federal, private sector, state and international partners can cooperate to respond to incidents. It also outlines the roles and responsibilities of the various agencies that may be involved in a response to an

CONTINUED ON PAGE 11

CONTINUED FROM PAGE 10

incident impacting critical infrastructure. Finally, the NCIRP contains a proposed classification and severity-level matrix, informing stakeholders how CISA intends to distinguish the lower-level "Baseline" incidents from higher-level "Severe" or "Emergency" incidents. The proposed NCIRP provides helpful insight into CISA's incident response and coordination priorities. Critical infrastructure entities should use the proposed NCIRP, and the forthcoming final version, to guide the ongoing review (or development) of their incident response plans and programs. Incident response planning is poised to remain a top regulatory concern for critical infrastructure in the coming months and years.

For more information on CIRCIA, visit **https://www.polsinelli.com/publications/critical-infrastructure-cybersecurity-evolving-incident-response-obligations-integral-to-effective-risk-management**

What Is Next for Critical Infrastructure Entities in the U.S.?

The focus of U.S. critical infrastructure cybersecurity regulation to date has been on information sharing and gathering, while the EU has already begun to regulate prophylactic security controls. EU policymakers will debate the distribution of risk, the burden of compliance and the improved readiness as these laws continue to take effect over the next year. Many suspect that U.S. lawmakers will wait to observe NIS2's impact on European critical infrastructure entities before making moves to implement similar broadly applicable legal frameworks.

For now, any **U.S. companies within critical infrastructure would be wise to focus on incident response planning and incident response readiness** – including the logging and monitoring (of people, processes and technology) necessary to enable quick detection of incidents – as this will likely be the first security domain with any real regulatory momentum in the states. If and when we do see more prescriptive security requirements in the U.S., they will likely simply codify well-established industry best practices, like those reflected in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Version 2.0) and CIS Critical Security Controls (Version 8.1). Any companies that have not already done so should go ahead and focus on building out and assessing their security programs to align with these frameworks.

Tell Me Lies: The Legal Risks Associated with Misrepresenting Data Security and Privacy

Starr Turner Drum
Shareholder
Los Angeles

Sarah S. Glover
Shareholder
Birmingham

Noor K. Kalkat
Associate
Los Angeles

> "If you make those claims without adequate support, you can expect to hear from the FTC."
>
> **Samuel Levine**
> Director of the Bureau of Consumer Protection, Federal Trade Commission

U.S. companies public and private across all industry verticals have come to use representations about technology, including the company's data security and privacy practices, as a marketing tool. Before touting the ways in which a company protects its systems and customer data, however, organizations would be well advised to appreciate the potential pitfalls.

The Risks

There are myriad ways a business can be held accountable for failing to do what it tells a customer it will do. Failing to abide by promises — contractual or otherwise — to secure data could lead to breach of contract or fraud claims, customer churn and reputational damage. Businesses should also be aware that there are governing statutory schemes and regulatory enforcement precedent directly on point when it comes to making misrepresentations about an organization's data security and privacy practices and should take steps to stay on the right side of the law.

FTC Enforcement

The Federal Trade Commission (FTC) is empowered under Section 5 of the FTC Act to "prevent persons, partnerships or corporations" from using "unfair or deceptive acts or practices in or affecting commerce." Section 5 does not explicitly mention data security or privacy. However, the FTC has long maintained its authority to go after companies that misrepresent the way they protect customer data to the public. This authority has been challenged, but unsuccessfully. The FTC's action against Wyndham Worldwide Corp. in 2012 solidified the commission's enforcement authority in this domain.[1]

The FTC's complaint against Wyndham alleged that Wyndham failed to take reasonable security measures to safeguard personal information, which resulted in substantial consumer injury when hackers obtained unauthorized access to Wyndham's computer networks on three separate occasions. On interlocutory appeal to the Third Circuit U.S. Court of Appeals, the court affirmed that the FTC has authority to regulate data security.

Since Wyndham, the FTC has pursued hundreds of data security and privacy actions under Section 5 across a number of industries, including against social media companies; application developers; data brokers; ed tech, ad tech and health tech companies; online retailers; and companies in the Internet of Things (IoT) space. All these actions essentially boil down to one or two things: (1) you don't do what you say and/or (2) you don't adequately protect data. Many findings have resulted in up to 10-figure penalties and 20-year consent decrees against companies the FTC has prosecuted.

What makes a data security or privacy statement "unfair" or "deceptive"? The FTC will know it when it sees it.[2] Companies are encouraged to

[1] Complaint for Injunctive and Other Equitable Relief, *FTC v. Wyndham Worldwide Corp.*, 2012 WL 12146600 (D.N.J. 2012).
[2] An act or a practice is "unfair" if: 1) it causes or is likely to cause substantial injury to consumers; 2) the injury is not reasonably avoidable by consumers; and 3) the injury is not outweighed by benefits to consumers or competition. A practice is "deceptive" if: 1) a representation, omission or practice misleads or is likely to mislead the consumer; 2) a consumer's interpretation of the representation, omission or practice is considered reasonable under the circumstances; and 3) the misleading representation, omission or practice is material.

CONTINUED ON PAGE 13

CONTINUED FROM PAGE 12

heed lessons learned from prior enforcement actions. Here are noteworthy examples of actions prosecuted as unfair or deceptive by the FTC over the years:

- Failing to implement patch management policies and procedures to ensure timely remediation of critical security vulnerabilities and using obsolete (end-of-life (EOL)) versions of database and web server software;[3]
- Representing that the company provides end-to-end data encryption but failing to do so in certain instances;[4]
- Representing that the company uses standard security practices but failing to test or review security features and failing to conduct regular risk assessments, vulnerability scans and/or penetration testing of its networks and databases;[5]
- Failing to have a policy or procedure for inventorying and deleting consumers' personal data stored on the company's network;[6]
- Failing to protect consumer personal data in the ways stated in a company's online privacy policy;[7]
- Presenting misleading public-facing statements to consumers about the anonymity of browsing data collected and sold;[8]
- Retaining voice recordings after advising consumers that they had been deleted and could request deletion at any time;[9]
- Sharing personal health information with advertisers despite a privacy notice promise to never do so.[10]

The FTC has stated in the context of misleading and deceptive advertising that it does not pursue subjective claims or "puffery" — claims such as "this is the best hairspray in the world."[11] However, if there is an objective component to the claim, such as "more consumers prefer our hairspray to any other" or "our hairspray lasts longer than the most popular brands," then the company will need to make sure it has adequate substantiation before making the claim. This is especially true in the case of representations about data security and privacy because the consequences can be significant. If a hairspray company doesn't live up to the hype, consumers may experience frizz. If a company fails to protect personal data, consumers may experience identity theft.

SEC Enforcement

The FTC is not the only regulator to police this type of activity. The Securities and Exchange Commission (SEC) has recently flexed its muscle by bringing an enforcement action against SolarWinds Corp. and its chief information security officer (CISO) (collectively, the defendants) after SolarWinds sustained a massive supply chain attack in 2020 affecting its flagship security software platform. The software was compromised after attackers injected malicious code into an application before it was put into operation at thousands of companies and government agencies. The SEC alleged that the defendants "defrauded SolarWinds' investors and customers through misstatements, omissions and schemes that concealed both the Company's poor cybersecurity practices and its heightened — and increasing — cybersecurity risks."

Among other claims, the SEC alleged that SolarWinds made false and misleading statements in its public-facing website material as well as its press releases, blog posts and podcasts. Chiefly, SolarWinds maintained a "Security Statement" on its website that summarized its data security program — a not uncommon feature of many software and technology company websites. The SEC alleged that the following representations were revealed to be fraudulent in light of the cyberattack: 1) that SolarWinds adhered to the National Institute of Standards and Technology (NIST) Cybersecurity Framework; 2) that the company developed its software using a secure software development life cycle (SSDLC); and 3) that the company implemented and maintained adequate network monitoring, password protocols and

[3] In the Matter of CafePress, available at https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter
[4] In the Matter of Zoom Video Communications, Inc., available at https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint_0.pdf
[5] In the Matter of Drizly, available at https://www.ftc.gov/legal-library/browse/cases-proceedings/2023185-drizly-llc-matter
[6] *Id.*
[7] In the Matter of Chegg, Inc., available at https://www.ftc.gov/system/files/ftc_gov/pdf/Chegg-Complaint.pdf
[8] In the Matter of Avast Ltd. et al., available at https://www.ftc.gov/system/files/ftc_gov/pdf/202_3033_-_avast_final_consent_package.pdf
[9] *U.S. v. Amazon.com, Inc.*, available at https://www.ftc.gov/system/files/ftc_gov/pdf/1923128amazonalexaorderfiled.pdf
[10] *U.S. v. GoodRx Holdings, Inc.*, available at https://www.ftc.gov/system/files/ftc_gov/pdf/goodrxfinalstipulatedorder.pdf
[11] Myths and Half-Truths About Deceptive Advertising (October 15, 1996), available at https://www.ftc.gov/news-events/news/speeches/myths-half-truths-about-deceptive-advertising

CONTINUED ON PAGE 14

CONTINUED FROM PAGE 13

access controls. The SEC alleged that the defendants knew the company had experienced "widespread and persistent failures" in each of these security areas that went to the heart of its products as a security company, thereby making them material to investors.

The backlash to the SEC's claims has been loud — industry experts and practitioners are concerned about a "chilling effect" on the dissemination of information about security and privacy, and especially on the ability of CISOs and other technology leaders to adequately perform their jobs for fear of being held personally responsible for a data security incident.

Litigation

Privacy- and cybersecurity-focused litigation has skyrocketed during the past few years. **Between 2021 and 2023, the volume of complaints referencing "ransomware" increased by more than 600% and the volume of complaints referencing "data breach" increased by more than 200%.** These lawsuits will often fold in consumer protection claims that allege defendants made misrepresentations about how they would treat personal information.[12]

The more explicit companies are about the ways in which they will safeguard consumer information, the more fodder for the plaintiffs' bar when those protections fail. What may have initially seemed like a great, marketing-focused commitment to safeguard consumer personal data can quickly become a pre-written checklist of security and privacy commitments that the organization allegedly failed to honor.

The Guidance

It goes without saying that any contractual requirements regarding data security and privacy should be thoroughly reviewed by the appropriate legal and technical subject matter experts. Most companies, however, do not deploy the same level of diligence when it comes to marketing and other public-facing material about data security and privacy — and they need to, in light of the authority cited above.

There are a number of stakeholders across an organization that may touch or weigh in on public-facing representations about data security and privacy — marketing, legal/compliance, IT/security, customer relations, product development, etc. Businesses need to deploy adequate review and approval protocols across these stakeholders to govern any statements about the organization's data security and privacy practices. Failure to do so can result in the unintentional and/or negligent publication of false and misleading statements that introduce legal risk to the organization. Below are action items and guidelines to help reduce this risk:

- Develop a website content development policy and procedure.
- When selecting material (existing or new) for the website, accuracy trumps everything else.
- Avoid unqualified statements that leave no room for exceptions. Most organizations could not stand by the bald statement "We encrypt all data" without qualification.

[12] *See, e.g., Atkinson v. Minted, Inc.*, 2020 WL 3254373 (N.D. Cal.); *Hyunh v. Quora, Inc.*, 2020 WL 1921875 (N.D. Cal.); *Flores-Mendez v. Zoosk, Inc.*, 2022 WL 19038559 (N.D. Cal.).

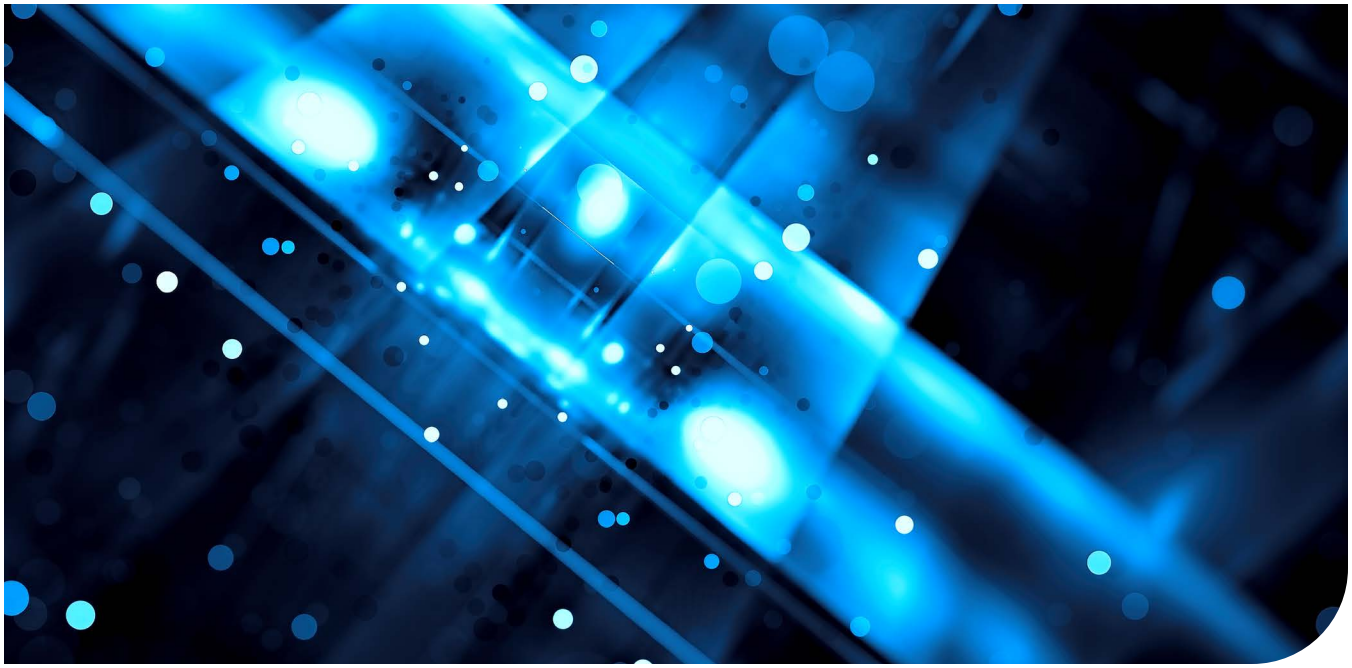
CONTINUED ON PAGE 15

CONTINUED FROM PAGE 14

- Avoid absolutes. Companies should always avoid using the word "always" in this content and should never use the word "never."
- Avoid guarantees. There are no guarantees when it comes to data security and privacy. You cannot "100% guarantee" that you can keep data secure — nobody can or should make this representation.
- Don't make promises you can't keep. For example, don't tell customers you will delete their data upon request or within 30 days following termination if your organization has not deployed adequate protocols to reasonably ensure that this in fact happens.
- Less is more. Detailed technical details are inappropriate for public-facing marketing content. Save that for product specs and terms and conditions.
- Public-facing information about data security and privacy must be reviewed by legal and compliance subject matter experts.
- Public-facing information about data security and IT must be reviewed by the internal IT subject matter experts as well.
  - Note that a company's IT systems and security controls change frequently — what was true two years ago may no longer be accurate. The regular review of existing content — not just net new content — is important.
- Legal and marketing professionals alike know that terminology matters and descriptive words should be chosen carefully.
  - For example, if you state that your company deploys "military grade" security, that could be misinterpreted as erroneously implying that a company's products are compliant with federal defense contracting standards (e.g., the Federal Acquisition Regulations System/ Defense Federal Acquisition Regulation Supplement).

The Takeaway

Ten-plus years ago, touting your strong cybersecurity and privacy practices may have been a market differentiator. Today, keeping data secure and upholding well-established privacy principles is table stakes. Organizations that do not do what they say they do can and will be held accountable — by their customers, by their industry, by the plaintiffs' bar and by regulators. As with cybersecurity and privacy generally, this is not just a marketing issue or an IT issue or a legal issue. Cybersecurity and privacy risk is an enterprise risk and must be addressed holistically and consistently.



2024 State Consumer Privacy Law Year-in-Review

Alexander S. Altman
Counsel
San Francisco

Elizabeth Snyder
Associate
New York

It was a busy year for state legislatures seeking to protect their residents' privacy. In 2024, seven states passed comprehensive consumer privacy laws: Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey and Rhode Island. At a high level, these states have not deviated greatly from their predecessors, with each:

- Obligating businesses to limit their processing of consumers' personal data to specific purposes;
- Imposing transparency obligations (e.g., providing consumers a compliant privacy notice or policy);
- Requiring businesses to recognize certain consumer rights, particularly with respect to access/portability, deletion and correction;
- Prohibiting or limiting the collection of "sensitive data" without consent;
- Requiring organizations to allow consumers to opt out of certain processing activities, such as the sales of personal data, targeted advertising and profiling or automated decision-making.

Each of these laws also exempts, with some variation, data or entities subject to the Health Insurance Accountability and Affordability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA) and other federal sectoral privacy laws.

Organizations already complying with the existing patchwork of state consumer privacy laws should be well positioned to comply with these new laws as they come into effect over the next two years. The devil, however, is in the details, and these new laws depart from existing state consumer privacy laws in novel ways. Below we summarize at a high level the fundamental aspects of these laws and some notable departures from other state consumer privacy laws, organized by each law's effective date. However, organizations that operate in these states will want to carefully analyze the new laws to identify any impact to their existing privacy compliance programs.

Nebraska — Effective Date: January 1, 2025

The Nebraska Data Privacy Act (the Nebraska Act) differs from most other state privacy laws — but aligns with Texas' consumer privacy law — in that it does not apply a threshold of processing activity to determine which entities are in scope. Rather, any entity doing business in the state is subject to the Nebraska Act. Along with other common exemptions, however, the Nebraska Act generally exempts small businesses, as defined by the Small Business Administration, with the exception of restrictions on sales of sensitive data without consumer consent, which all businesses must follow.

The Nebraska Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data.

New Hampshire — Effective Date: January 1, 2025

New Hampshire Senate Bill 255 (the New Hampshire Act) adopts a structure and thresholds similar to existing state privacy laws, applying to "controllers" that do business in New Hampshire and that, during a calendar year, either (1) control or process the personal data of at least 35,000 New Hampshire consumers, or (2) control or process personal data of 10,000 New Hampshire consumers and derive over 25% of gross revenue from the sale of personal data. Unusually, the 35,000-consumer threshold excludes "personal data controlled or processed solely for the purpose of completing a payment transaction."

The New Hampshire Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data and must honor consumers' revocation of such consent.

New Jersey — Effective Date: January 15, 2025

New Jersey Senate Bill 332 (the New Jersey Act) will apply to controllers that do business in New Jersey and, during a calendar year, either (1) control or process the personal data of at least 100,000 New Jersey consumers, or (2) control or process personal data of 25,000 New Jersey consumers and derive any revenue from the sale of personal data.

The New Jersey Act has no exemption for nonprofit organizations and, unlike

CONTINUED ON PAGE 17 ▸

CONTINUED FROM PAGE 16

most state consumer privacy laws, does not exempt data or entities subject to FERPA.

The New Jersey Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data and must honor consumers' revocation of such consent.

The New Jersey Act is atypical — joined only by California's and Colorado's laws — in that it provides for a regulatory framework, requiring the director of the Division of Consumer Affairs in the Department of Law and Public Safety to promulgate rules necessary to further the purposes of the act. The New Jersey Act does not impose a deadline for the promulgation of rules, so it remains to be seen when and how they may impact enforcement.

Minnesota — Effective Date: July 31, 2025

The Minnesota Consumer Data Privacy Act (the Minnesota Act) will apply to controllers that do business in Minnesota and, during a calendar year, either (1) control or process the personal data of at least 100,000 unique Minnesota consumers, or (2) control or process personal data of 25,000 unique Minnesota consumers and derive over 25% of gross revenue from the sale of personal data. Notably, the Minnesota Act also largely exempts small businesses (with the exception of restrictions on sales of sensitive data without consent). Like the New Jersey Act, the Minnesota Act does not have a blanket exemption for nonprofits. It does, however, exempt nonprofits that are established to detect and prevent insurance fraud.

The Minnesota Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data and honor consumers' revocation of such consent.

Interestingly, the Minnesota Act gives consumers the right to request the specific third parties to which a controller has disclosed the consumer's personal data. Almost all other state consumer privacy laws require only that controllers be transparent about the categories of third parties to which they have made disclosures. This could pose a substantial burden on some controllers.

Additionally, the Minnesota Act uniquely gives consumers the right to question the results of profiling. Specifically, Minnesota consumers have the right to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions the consumer might have taken to secure a different decision and the actions that the consumer might take to secure a different decision in the future. The consumer has the right to review the personal data used in the profiling. If the decision is determined to have been based upon inaccurate personal data, the consumer has the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

Maryland — Effective Date: October 1, 2025

The Maryland Online Data Privacy Act (the Maryland Act) will apply to controllers that do business in Maryland and that, during the preceding calendar year, (1) controlled or processed personal data of at least 35,000 Maryland consumers, or (2) controlled or processed personal data of 10,000 Maryland consumers and derived more than 20% gross revenue from the sale of personal data. Like the Minnesota Act, the Maryland Act does not broadly exempt nonprofit entities. Rather, it exempts only nonprofits that process personal data either to assist law enforcement agencies in investigating criminal or fraudulent acts relating to insurance or to assist first responders responding to catastrophic events.

The Maryland Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. The Maryland Act imposes unique obligations surrounding sensitive data, requiring controllers to adhere strictly to data minimization requirements and prohibiting the sale of sensitive data entirely, regardless of whether a consumer provides consent.

Kentucky — Effective Date: January 1, 2026

Kentucky's Consumer Data Protection Act (the Kentucky Act) will apply to controllers that do business in Kentucky, and that, during a calendar year, either control or process the personal data of at least (1) 100,000 Kentucky consumers, or (2) 25,000 Kentucky consumers and derived over 50% of gross revenue from the sale of personal data. The Kentucky Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data.

CONTINUED ON PAGE 18

CONTINUED FROM PAGE 17

Notably, unlike many recently enacted state privacy laws, the Kentucky Act will not require the businesses to recognize universal opt-out mechanisms (such as Global Privacy Controls or GPCs) to process requests to opt out of sales of personal data or targeted advertising.

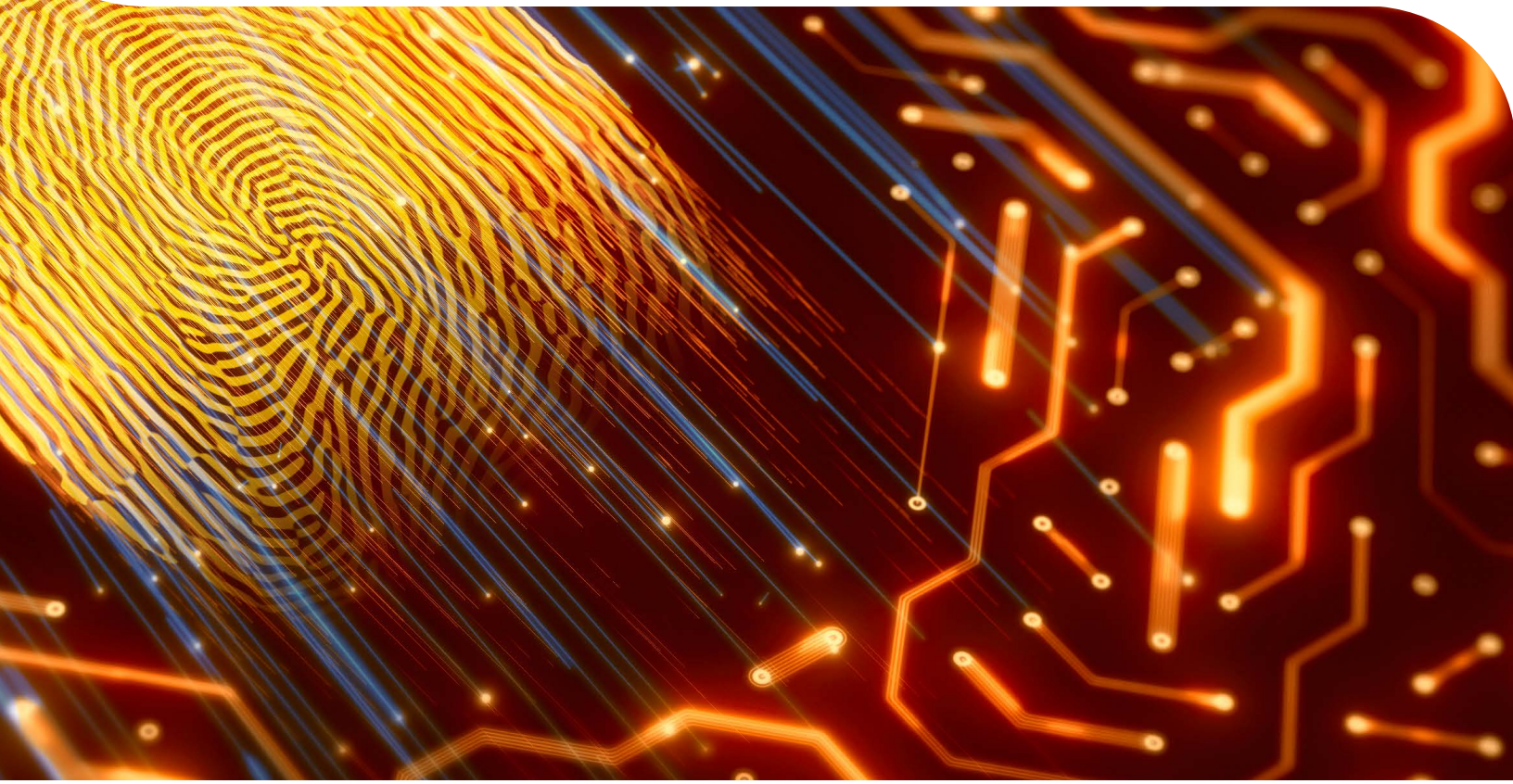
Rhode Island — Effective Date: January 1, 2026

The Rhode Island Data Transparency and Privacy Act (the Rhode Island Act) will apply to controllers that do business in Rhode Island and, during the preceding calendar year, either (1) controlled or processed the personal data of at least 35,000 Rhode Island consumers, or (2) controlled or processed personal data of 10,000 Rhode Island consumers and derived 20% of gross revenues from the sale of personal data.

The Rhode Island Act gives consumers the right to confirm whether a controller is processing their data; to correct, delete and obtain copies of their personal data; and to opt out of personal data sales, profiling and targeted advertising. Additionally, businesses must obtain consent to process sensitive data and honor consumers' revocation of such consent.

While the Rhode Island Act aligns with the other state privacy laws in effectively requiring controllers to provide consumers a privacy notice or policy, it sets a high bar for transparency with respect to the sales of personal data. Unlike most of the other state consumer privacy laws, but similar to the Minnesota Act, the Rhode Island Act requires controllers to identify all third parties — not merely "categories" of third parties — to which the controller has sold or "may sell" personal data.

In sum, 2024 saw a continuation of the past several years' trend in the passage of state consumer privacy laws. While these new laws are largely similar in scope, exemptions and obligations, they do have notable differences. As effective dates approach, organizations should review these new laws and their compliance programs to ensure that any differences are accounted for.



Recent Developments Relating to the SEC's Cybersecurity Disclosure Requirements

Eric S. Wu
Shareholder
Washington D.C.
Kansas City

Pavel (Pasha) A. Sternberg
Principal
Los Angeles

Mary Ann H. Quinn
Associate
Birmingham

The U.S. Securities and Exchange Commission (SEC) is becoming one of the federal agencies at the forefront of driving transparency, cybersecurity awareness and cyber incident reporting. As we reported in last year's publication, in 2023 the SEC implemented significant enhancements to cybersecurity-based disclosures for public companies (including new incident reporting requirements). The new incident reporting rule became effective for larger companies in December 2023 and has now been in force for an entire year. During this time, we observed the marked impact on public company decision-making while also noting the SEC's multifaceted enforcement of its more seasoned cybersecurity disclosure guidance that existed prior to 2023. This article summarizes our findings and experience over the past year guiding public companies affected by these changes.

Overview of the 2023 Rules

The SEC's new cybersecurity disclosure rules create more prescriptive data security incident disclosure and governance disclosure requirements, as follows:

1. **Form 8-K Disclosure of Material Cybersecurity Incidents.** The SEC added a new Item 1.05 to Form 8-K that requires companies to disclose a cybersecurity incident within four business days of the date such cybersecurity incident is determined to be material. The materiality standard is the same as for other required disclosures — information is material "if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision" or if it would have "significantly altered the 'total mix' of information made available." The SEC has also encouraged voluntary disclosure of cybersecurity incidents that are not material (or for which a materiality decision has not yet been made) in other ways besides the new 8-K Item 1.05.[1]

2. **Regulation S-K Disclosure of Cybersecurity Risk Management, Strategy and Governance.** The SEC added Item 106 to Regulation S-K, which requires disclosure in a registrant's annual report on Form 10-K of: (1) the registrant's processes — if any — for assessing, identifying and managing material risks from cybersecurity threats, and whether any risks from cybersecurity threats, including risks from previous cybersecurity incidents, have materially affected (or are reasonably likely to materially affect) the registrant, and (2) the Board's oversight of such risks and management's role in assessing and managing such risks. Under this requirement, registrants should provide investors with enough information for them to understand the registrant's cybersecurity practices but need not include a level of detail that could increase the registrant's vulnerability to future cyberattacks.

Recent Disclosure Trends

In the second half of 2024, a survey of approximately 80 SEC cybersecurity incident disclosures revealed some notable trends:

- Only ten of the surveyed filings reported a material cybersecurity incident under Item 1.05.
- Nearly 40 filings reported the incident was not material, showing that at least for now, public companies are following the SEC's recommendation to voluntarily disclose incidents even when they are not deemed material.[2]
- Significantly, approximately 30 filings reported a third-party/vendor incident.

Recent Enforcement Actions

1. The SEC Brings an Internal Accounting Control Claim, June 18, 2024

In June 2024, R.R. Donnelley & Sons, Co. (RRD) agreed to a $2.125 million civil penalty. The SEC charged RRD with security and disclosure failures related to a 2021 ransomware

[1] "Disclosure of Cybersecurity Incidents Determined to Be Material and Other Cybersecurity Incidents" (May 21, 2024), https://www.sec.gov/newsroom/whats-new/gerding-cybersecurity-incidents-05212024

[2] We believe that some of these voluntary filings are being made out of an abundance of caution while practitioners become more experienced with the Item 1.05 materiality determination and, at least in part, to avoid allegations that a material incident was not timely reported.

CONTINUED ON PAGE 20

CONTINUED FROM PAGE 19

incident. The SEC found that RRD's business was so critically dependent on storing and transmitting large amounts of potentially sensitive customer data that the SEC broadly deemed the company's information technology (IT) systems and networks to constitute "assets" requiring "sufficient accounting controls" under Section 13(b)(2)(B) of the Securities Exchange Act of 1934 (Exchange Act). The SEC specifically criticized the company's handling of its internal alert process and indicated that the staff tasked with reviewing security alerts was insufficient, had ill-defined roles and responsibilities and lacked clear criteria for alert prioritization and workflows.

Two SEC commissioners published a public dissent of this settlement order, saying that including IT systems in "accounting controls" was an overreach that unfairly allowed the SEC to regulate public companies' cybersecurity practices.[3] These dissenters noted that the SEC had begun to treat the accounting controls provision of Section 13(b)(2)(B) like a "Swiss Army Statute to compel issuers to adopt policies and procedures the Commission believes prudent," but that doing so "distort[ed] a statutory provision" to "punish a company that was the victim of a cyberattack."[4] The dissent also maintained that RRD's "information technology systems and networks" do not fit the category of assets intended to be captured by Section 13(b)(2)(B).

2. The SEC's Federal Case Against SolarWinds Corporation (SolarWinds) and Its CISO Is Largely Dismissed, July 18, 2024

The SEC filed a complaint in the Southern District of New York (SDNY) on October 30, 2023, against SolarWinds and its chief information security officer (CISO), Timothy Brown, with claims arising from disclosures the company made about its cybersecurity practices and the massive cyberattack the company suffered in 2020. The filing of the case itself marked a new era in the SEC's enforcement of cybersecurity disclosure practices. The SEC alleged SolarWinds committed securities fraud, made materially misleading disclosures, had ineffective internal accounting controls and had ineffective disclosure controls. Notably, this was the first time the SEC brought to federal court its claim for ineffective accounting controls based on cybersecurity controls such as password and VPN protocols.

On July 18, 2024, the SDNY dismissed most of the SEC's claims against SolarWinds and its CISO.[5] The SDNY emphasized that "perspective and context are critical" and did not find any material misstatements in SolarWinds' SEC filings (but did permit a claim related to SolarWinds' website disclosure).[6] The SDNY also soundly dismissed the SEC's accounting controls claim, finding that Section 13(b)(2)(B) of the Exchange Act was clearly meant to cover only financial accounting

[3] Commissioners Hester M. Peirce and Mark T. Uyeda, "Statement on R.R. Donnelley & Sons, Co." (June 18, 2024), https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-rr-donnelley-061824

[4] *Id.*

[5] *Sec. & Exch. Comm'n v. SolarWinds Corp.*, No. 23 CIV. 9518 (PAE), 2024 WL 3461952 (S.D.N.Y. July 18, 2024).

[6] *Id.* at *44.

CONTINUED ON PAGE 21

CONTINUED FROM PAGE 20

controls, not cybersecurity.[7] As a result, the decision may shift the SEC's enforcement approach going forward, in and out of federal court.

3. The SEC Settles With Four Additional Companies for SolarWinds Disclosures, October 22, 2024

On October 22, 2024, the SEC settled with four current or former publicly traded companies for disseminating materially misleading disclosures regarding cybersecurity risks and incidents. Unlike the SolarWinds complaint, these four settlements did not involve any accounting controls claims. Each of these four cases arose from an investigation of companies impacted by the 2020 cyberattack on SolarWinds. The SEC alleged that each of the four companies violated Section 13(a) of the Exchange Act, as amended, as well as the respective rules promulgated thereunder that require public companies to file annual, quarterly and current reports in conformity with the SEC's rules and regulations. The SEC alleged that each of the four companies learned in either 2020 or 2021 that the perpetrator of the SolarWinds attack had also infiltrated their own systems, but in their respective 2021 and/or 2022 disclosures, each company negligently minimized the cybersecurity incident. The SEC found this particularly concerning because the SolarWinds incident compromised each of the four companies' core business functions — enterprise IT services. The companies agreed to settle the SEC's charges as follows:

- Company A agreed to a **$990,000 civil penalty**. In multiple Forms 8-K filed in 2021, Company A minimized the severity of the attack on it by, among other things, failing to disclose the quantity of encrypted credentials accessed by the threat actor.
- Company B agreed to a **$1 million civil penalty**. Company B disclosed in a Form 10-Q filed in February 2021 that the threat actor had accessed a limited number of email messages; in reality, Company B was already aware the threat actor accessed over 100 files in its cloud file-sharing environment.
- Company C agreed to a **$995,000 civil penalty.** Even though Company C was aware of the intrusion, it described cyber intrusions and related risks in a generic fashion in its Annual Reports on Form 20-F filed in both 2021 and 2022.
- Company D agreed to a **$4 million civil penalty**. Company D described its risks from hypothetical future cybersecurity events in its Annual Reports on Form 10-K filed in both 2021 and 2022, even though it was aware it had already experienced two intrusions related to SolarWinds. In addition, the SEC charged Company D with violations relating to disclosure controls and procedures, resulting in such materially misleading disclosures.

While the SEC's 2023 disclosure rules were not in effect at the time of these four companies' alleged violations, these settlements demonstrate that the SEC has been increasingly aware of and focused on enforcing sufficient and appropriate cybersecurity disclosures.

Where Might the SEC Be Trending?

The SEC Staff has reiterated across multiple forums its position that, although public companies may be victims of cyberattacks, they may not in turn harm their shareholders or the investing public by issuing misleading disclosures about cybersecurity incidents, controls, or overall risk. Moreover, it is clear that the SEC has increased its cybersecurity vigilance in recent years. In its 2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosure (SEC Release Nos. 33-10459; 34-82746), the SEC's interpretive guidance specified that ". . . if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur. . . . Instead, the company may need to discuss the occurrence of that cybersecurity incident and its consequences. . . ." The SEC's 2023 rulemaking and recent enforcement actions illustrate its continued focus on public companies disclosing cybersecurity incidents as well as accurately and specifically reporting cybersecurity risks. In particular, it is quite possible that the SEC's recent trend of scrutinizing cybersecurity disclosures may extend to the Form 8-K Item 1.05 requirement to disclose a material cybersecurity incident within four business days of a materiality determination. As such, public companies should review their disclosure controls and procedures to confirm their effectiveness in enabling compliance with the SEC's cybersecurity disclosure rules in connection with future cybersecurity incidents that may impact them directly or indirectly.

[7] *Id.* at *48-52.

Threat Actor Trends and Practical Guidance — A Conversation Between Polsinelli and Coveware

Alexander D. Boyd
Shareholder
Kansas City

Jessica L. Peel
Associate
Kansas City

Anna K. Schall
Associate
Kansas City

As cybersecurity professionals know all too well, threat actors continue to evolve in order to overcome organizations' defenses. However, by analyzing these threats and trends, organizations can take steps now to further reduce their risk and to better prepare to respond when an incident occurs.

Coveware is a leading cyber extortion incident response firm that helps victims recover encrypted or stolen data as a result of a cyberattack. Polsinelli and Coveware have partnered for many years in helping organizations of all sizes and industries navigate cyber extortion and ransomware attacks. To help organizations prepare for the upcoming year, Polsinelli spoke with Coveware regarding threats and trends observed in 2024 and predictions for 2025. Based on these threats and trends, organizations can take steps to further reduce the risk of incidents and to better prepare to respond to an incident if one occurs.

There is little, if any, data indicating that certain industries are more at risk than others for a cyberattack. Accordingly, all businesses continue to be at risk and should prepare for when (not if) a cyberattack will happen.

All organizations should follow a layered approach to address this risk:

- Reducing the risk of an incident through risk assessments, technical security measures, training and vendor vetting;
- Reducing the scope of a potential incident through record retention and deletion policies, data mapping and segmentation;
- Preparing to effectively respond to an incident with updated and exercised incident response plans.

Although all entities are at risk for a cyberattack, the type of attack and the root cause of the attack can vary by entity size. Threat actors continue to exploit known software vulnerabilities to infiltrate small and medium-sized businesses. The threat actors can easily identify organizations that are vulnerable to these attacks, and smaller organizations often lack sophisticated patching programs that address the frequent patches and updates necessary to address this risk. Threat actors are also likely to continue both exfiltrating and encrypting data during a ransomware attack on a small-to-medium-sized business.

In contrast, threat actors are increasingly choosing to steal data from larger organizations without also encrypting the data in the attack in order to further delay detection and to reduce their profile with law enforcement. Threat actors are also more likely to invest in more sophisticated social engineering attacks for these larger organizations. While large businesses often implement employee training to identify traditional phishing emails, threat actors are now leveraging artificial intelligence to launch more sophisticated and targeted attacks using advanced data analytics coupled with highly convincing voice phishing ("vishing") schemes.

For example, a threat actor may call an employee from a spoofed number, appearing to be from a member of the IT department, regarding a network problem or routine maintenance project, then confirm the name of the employee's manager and ask the employee to perform a simple task over the phone. During that task, the threat actor is granted access to the employee's computer and is able to install malware for remote access, move laterally within the environment, steal data or otherwise cause damage. Organizations should ensure that their training programs include multiple avenues for phishing, including email, text and phone calls.

Both large and small organizations are also increasingly falling victim to search engine optimization (SEO) poisoning or "malvertising" where the threat actor has tricked an employee (even an IT professional) into downloading and installing malicious software designed to look like a known legitimate tool. They achieve this by registering domains to host malicious payloads and increasing the prominence of such

CONTINUED ON PAGE 23 ▸

CONTINUED FROM PAGE 22

domains so they appear high up in the list of search engine results, thereby feigning credibility and authenticity. Organizations should ensure that internal and external IT personnel are using only vetted tools from approved sources. Threat actors also continue to specifically target external managed service providers (MSPs). Organizations should appropriately vet all vendors, including MSPs, and ensure that their contracts address cybersecurity requirements and data incident notifications and responsibilities.

"Phantom demands" also increased for all businesses in 2024, and it is expected they will continue to take place through 2025. A phantom demand occurs when a threat actor claims to have infiltrated an organization's network and/or stolen an organization's data but has not actually done so. Threat actors typically provide phantom demands via email, and they fall into two main categories:

- An entity was not actually attacked, and the threat actor makes a low monetary demand with the hope that payment will be made without due diligence.
- The entity or a third party that holds the entity's data experienced a data security event within the preceding several years, and the threat actor discovered stale information from those incidents on the dark web.

The first type of phantom attack has been occurring for years; however, the second type (the legacy extortion event) is becoming more frequent. We believe this trend is the result of combined circumstances, including a shrinking victim landscape, increasingly desperate economics for extortion actors and the availability of artificial intelligence to easily data mine large datasets from prior incidents.

Lastly, between 2023 and 2024, federal and international law enforcement made significant progress in investigating, identifying and disrupting large ransomware groups, their ecosystems and their resources. As a result, market share is no longer held by two to three large ransomware-as-a-service (RaaS) syndicates. Instead, the landscape is populated by a few legacy groups that strive to maintain a small footprint, a handful of "new" variants that have emerged following the collapse of others, and a decentralized collection of lone actors who likely came from prior RaaS organizations but have struck out on their own now that being linked to a group appears to carry more risk than reward compared to years past. These newer groups and lone threat actors often act in less predictable ways following an attack. This means that organizations may have less information available to them during communications with the threat actor. For example, there will be less information known about whether the threat actor will actually provide a decryption key in exchange for payment, whether the threat actor will negotiate and whether the threat actor will still publish leaked data even after payment is made. Decryption tools from smaller groups can also be less reliable. As a result, it is even more important for organizations to do everything they can to reduce the risk of an attack and to ensure that they have recent, viable backups if an attack does occur.

While no organization can prevent all potential cyberattacks, a comprehensive cybersecurity, resiliency and incident response program can reduce the risks associated with these attacks. By analyzing and forecasting threat actor trends, organizations can put themselves in the best position to address these evolving risks.

Current Trends in Data Breach Notification Laws: Safe Harbors and Reinforcing the Case for Cybersecurity

Adam Griffin
Shareholder
Washington, D.C.

Todd Panciera, Jr.
Associate
Birmingham

Sara Kopetman
Associate
Ft. Lauderdale

The early 2000s marked the start of a new era for consumer protection with the passage of the data breach notification law in California, the first of its kind. Since that time, a patchwork of privacy laws has been enacted across the United States, signaling an ever-greater regulatory shift toward consumer privacy protection. And since the passage of the comprehensive California Consumer Privacy Act of 2018 (CCPA), the United States has seen exponential growth in the number of privacy-related bills being introduced in state legislatures (59 in each of the past two years) as well as the number of bills being passed into law (7 in 2023).[1] This surge in legislative activity has led to a significant increase in both consumer data privacy protections and data breach litigation. This article will first provide a brief update on the state data breach notification laws. Next, it will explore how legislatures and courts are navigating the uptick in data privacy litigation and what the implications are for businesses facing both increased regulation and rising litigation risks.

Updates to State Data Breach Notification Laws

State legislatures continue to update existing data breach notification laws to infuse greater consumer privacy protections. For example, recent updates in Pennsylvania, Florida and Utah add new requirements for companies reporting data breaches, requiring companies to provide complimentary credit monitoring services when certain information is affected (Pennsylvania), increasing regulatory reporting requirements (Pennsylvania and Utah), and expanding the scope of reportable information to include new categories of personal data, including biometric and geolocation data (Florida).

Increased Consumer Litigation

The volume of data breach class action litigation is also growing at a remarkable rate. According to a July 2024 report by Lex Machina,[2] the number of data breach class action cases filed in 2023 nearly tripled the number of such class actions filed in 2022. In fact, in 2023, an average of 170 data breach class actions were filed each month. The total number of data breach class actions filed in the past three years has grown exponentially from just 476 in 2021 to 2,040 in 2023, according to Lex. This increase is believed to be due in part to recent court decisions making it easier for plaintiffs to show standing and successfully prove causation. Just given the volume of such cases handled by our firm in 2024, we expect this growth to continue.

Safe Harbor Provisions

In light of the uptick in data privacy laws favoring consumers and perhaps in response to the exponential increase in data breach class actions, a growing number of state legislatures and courts appear to be attempting to rebalance the scales by creating more favorable outcomes for businesses working to bolster cybersecurity in favor of consumers. This apparent shift away from unnecessarily penalizing businesses who are themselves victims, particularly in cases where actual consumer harm has not occurred, should promote a fairer legal environment. Ohio has led the way as the first state to pass a Safe Harbor provision in 2018 with the passage of its Data Protection Act (DPA). Ohio's DPA provides an affirmative defense in tort-based data breach claims for businesses that implement cybersecurity programs meeting industry-recognized cybersecurity frameworks. According to the legislative notes, the Ohio legislature's aim in writing the law was in part to reduce the likelihood of potential class actions and streamline the court's docket with respect to

[1] *U.S. State Comprehensive Privacy Laws Report*, IAPP (October 2024) (available at https://iapp.org/resources/article/us-state-privacy-laws-overview/?utm_source=Google&utm_medium=Paid&utm_campaign=StatePrivacy&utm_content=&gad_source=1&gclid=CjwKCAiA9IC6BhA3EiwAsbltOFaJudRWwJSBDkJD38JTKfn3Z2ixaVaSTqUtFm37OjALTcwaxxp4phoCpOAQAvD_BwE).
[2] Laura Hopkins et al., *Lex Machina Consumer Protection Litigation Report 2024* (July 2024) (available at https://pages.lexmachina.com/2024-Consumer-Protection-Report_LP.html).

CONTINUED ON PAGE 25

CONTINUED FROM PAGE 24

these matters (i.e., a "legal safe harbor" for compliant businesses)[3] while simultaneously elevating the cybersecurity standards of Ohio businesses.[4]

Tennessee passed a similar law that will go into effect on July 1, 2025. Under Tennessee's Safe Harbor, a private entity is not liable in a class action lawsuit resulting from a cybersecurity event unless the cybersecurity event was caused by willful and wanton misconduct or gross negligence on the part of the private entity.[5]

In Florida, a similar bill passed both the House and the Senate but was ultimately vetoed by Gov. DeSantis.[6] The bill would have shielded an entity from liability in connection with cybersecurity incidents if the entity substantially complied with Florida's data breach notification requirement and adopted a cybersecurity program that substantially complied with several third-party frameworks specified in the bill.[7] In vetoing the bill, DeSantis expressed concern over whether the bill's "minimum cybersecurity standards" could "result in Floridians' data being less secure" and "incentiviz[e] doing the minimum when protecting consumer data."[8] DeSantis invited "interested parties to coordinate with the Florida Cybersecurity Advisory Council to review potential alternatives to the bill that provide a level of liability protection while also ensuring critical data and operations against cyberattacks are protected as much as possible."

Similarly, in West Virginia, Gov. Justice vetoed[9] a bill that, if passed, would have provided entities with an affirmative defense in tort actions alleging that personal information was breached because of an entity's failure to implement reasonable information security controls. For entities to be protected under the bill, they would need to adopt cybersecurity programs meeting the bill's specific requirements or certain industry-specific frameworks outlined in the bill. In vetoing the bill, Justice highlighted the "potential for bad actors to abuse this law and to harm [West Virginia] citizens" and invited stakeholders to help craft a bill that will help the state's businesses while protecting its citizens.

What is clear from these new safe harbor provisions, including those that have failed to pass, is that state governments continue to look for new ways to incentivize U.S. companies to improve consumer privacy standards without unduly burdening businesses that are victimized by increasingly sophisticated cybersecurity threats.

---

[3] Fiscal Note & Local Impact Statement, Ohio Legislative Service Commission (September 2018) (available at https://www.legislature.ohio.gov/download?key=10235).
[4] https://search-prod.lis.state.oh.us/api/v2/general_assembly_132/legislation/sb220/00_IN/pdf/
[5] T.C.A. § 29-34-215(b).
[6] CS/CS/HB 473: Cybersecurity Incident Liability, The Florida Senate (available at https://www.flsenate.gov/Session/Bill/2024/473/?Tab=VoteHistory).
[7] *See FL H.B. 473.*
[8] R. DeSantis, letter to Sec. of State Byrd (June 26, 2024) (available at https://www.flgov.com/eog/sites/default/files/press/Veto-Letter_HB-473.pdf).
[9] J. Justice, letter to Sec. of State Warner (March 27, 2024) (available at https://www.wvlegislature.gov/Bill_Text_HTML/2024_SESSIONS/RS/veto_messages/HB5338.pdf).

CONTINUED ON PAGE 26

CONTINUED FROM PAGE 25

Finally, the same may be said for the courts, which have begun raising the pleading standard in data breach class action cases to address the increasing number of actions being filed in which no cognizable injury has occurred. Certain courts[10] are requiring plaintiffs to demonstrate actual harm, such as financial loss, identity theft or other tangible damage, rather than merely speculative or hypothetical damage, in cases where personal information has been compromised. This change reflects a departure from prior case law[11] wherein the potential for identity theft and the mere exposure of personal data were sufficient to establish standing. This heightened standing requirement is reshaping the legal landscape for data breach claims and serves as a counterbalance to the rising tide of consumer protection laws, ensuring that businesses are not unjustly penalized for every potential vulnerability or data exposure and returning the focus to the ways companies can act, or in some cases react, to prevent or mitigate actual harm to consumers.

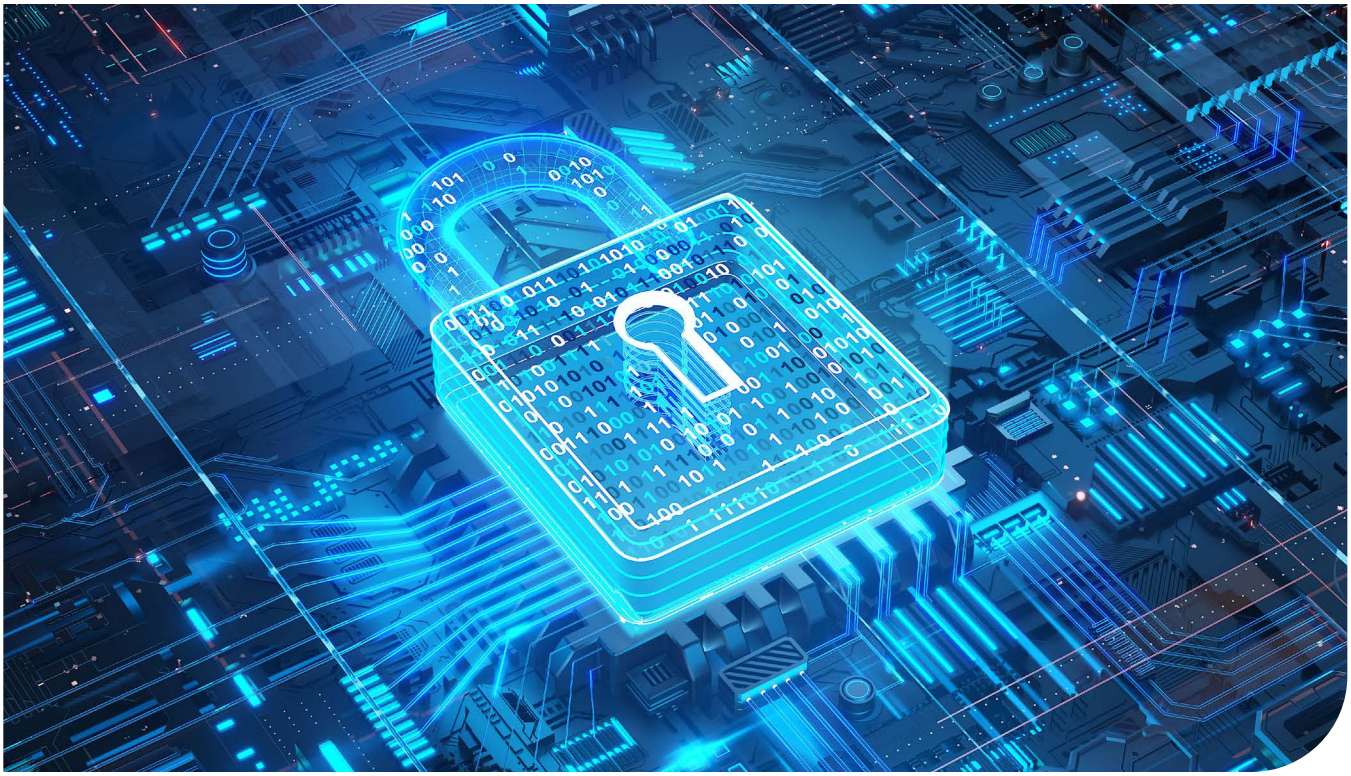
Takeaway for Companies: The Case for Investing in Cybersecurity

While a company's regulatory obligations may evolve as laws change, one constant is clear: Proactively investing in cybersecurity is always a smart business decision, particularly with the introduction of safe harbor provisions. Although not universal, the trend of courts attempting to limit data breach actions signals a shift in the legal landscape. With legislation and the courts not fully aligned with consumer interests, businesses have an opportunity to improve their standing by demonstrating a commitment to cybersecurity — making a strong case for themselves in the eyes of regulators and the public.

---

[10] Including federal courts in the 3rd, 4th, 8th and 11th circuits. *See Reilly v. Ceridian Corp.,* 664 F.3d 38, 42 (3rd Cir. 2011); *Beck v. McDonald,* 848 F.3d 262, 274–75 (4th Cir. 2017); In re SuperValu, Inc., 870 F.3d 763, 770 (8th Cir. 2017); *Tsao v. Captiva MVP Rest. Partners, LLC,* 986 F.3d 1332, 1333–24 (11th Cir. 2021).

[11] *See Attias v. Carefirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 387-89 (6th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC,* 794 F.3d 688, 692, 694-95 (7th Cir. 2015); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142-43 (9th Cir. 2010).



Beyond the Blockchain: What's Next for Digital Assets After Explosive Growth in 2024

Jonathan E. Schmalfeld
Associate
St. Louis

Ephraim T. Hintz
Associate
Los Angeles

Kaitlyn N. Robles
Associate
Los Angeles

Web3 represents the next evolution of the internet, characterized by decentralized networks and blockchain technology, enabling user-centric platforms and applications with enhanced security and data ownership. Digital assets, a cornerstone of Web3, include cryptocurrencies, non-fungible tokens (NFTs) and other blockchain-based assets, offering novel methods of value exchange, investment and digital ownership. Every other week, Polsinelli puts out its BitBlog Bi-Weekly,[1] which breaks down the biggest legal developments in the blockchain, Web3 and crypto industry over the two preceding weeks.

2024 was a landmark year for the Web3 industry, with its usage reaching all-time highs in volume and growing in total market cap from $1.7 trillion at the beginning of 2024 to roughly $3.5 trillion at the time of this writing. As we look back through 2024, the Web3 legal developments from the past year emphasize the critical need for clarity and balance in how laws and regulations intersect with emerging technologies.

Looking forward to what's next, a picture emerges of what legal trends companies looking to explore blockchain-enabled technologies and existing Web3 industry participants should pay close attention to in 2025.

Expected Shift in U.S. Regulatory Environment

With the change in presidential administrations, many are expecting to see a shift in how regulatory agencies and legislative efforts approach blockchain-enabled technologies. At the Securities and Exchange Commission (SEC), Chair Gary Gensler has announced his resignation, as has Commissioner Jaime Lizárraga; both voted to reject an application for a Bitcoin exchange-traded fund (ETF) before its eventual approval after the D.C. Circuit ruled the SEC's rejection was arbitrary and capricious. That leaves just Commissioners Peirce (seen as pro-crypto), Uyeda (pro-crypto) and Crenshaw (seen as anti-crypto, but on an expired term) left until new commissioners are appointed by President-elect Donald Trump and approved by Congress, including Paul Atkins, whom Trump has announced is his pick for next SEC chair.

Trump has also indicated he plans to shift certain administrative priorities involving digital assets away from the oversight of the SEC and under the umbrella of the Commodity Futures Trading Commission (CFTC). This indicates that the incoming administration believes most digital assets should be regulated as commodities instead of securities.

It also appears that David Sacks, who was announced to be the administration's artificial intelligence and cryptocurrency "czar," will have a significant role in the incoming administration's coordination of digital asset policies across agencies. It is unclear what that means for pending lawsuits brought by the SEC against major digital asset exchanges and how those existing enforcement actions will be handled with this shift in enforcement priorities.

Equally important will be whom Trump taps to lead the Department of the Treasury and to key positions in the Department of Justice. Already, Jay Clayton has been announced as the pick to lead the U.S. Attorney's Office for the Southern District of New York, with a corresponding announcement from the office's co-chief of the securities and commodities fraud task force that digital asset-related prosecutions are expected to be deemphasized in 2025.

On the legislative front, there is a real possibility for various digital asset legislative efforts to be passed in 2025. In 2024 the Financial Innovation and Technology for the 21st Century Act (FIT 21) passed in the House of Representatives with a substantial bipartisan 279-136 vote. There is a chance for comprehensive digital asset regulations to pass in the upcoming Congress, but it is expected the industry will advocate for something closer to the Safe Harbor proposal of Pierce (Proposed Securities Act Rule 195) rather than rushing to comprehensive legislation like FIT 21, which may have unanticipated downstream effects on future developments. There is also the expected legislation over "stablecoins"

[1] https://www.polsinelli.com/polsinelli-bitblog/category/bi-weekly-update

CONTINUED ON PAGE 28

CONTINUED FROM PAGE 27

(digital assets pegged to the U.S. dollar), discussed below, and various banking laws that are expected to come under scrutiny in the incoming Congress. All these changes are expected to help grow the digital asset industry in the United States, which had been shrinking in terms of market share in recent years due to various legal uncertainties and the risk of seemingly arbitrary enforcement actions.

Stablecoins Go Mainstream in 2025

A stablecoin is a type of cryptocurrency that is designed to provide the benefits of other cryptocurrencies (e.g., Bitcoin and Ethereum), such as fast transactions and decentralization, while maintaining a stable value over time and minimizing the volatility that is generally associated with cryptocurrencies. This stability is a result of the stablecoin being "pegged" (i.e., having its market value linked to an external reference) to a reserve asset, including fiat currencies (e.g., the United States dollar) or commodities (e.g., gold or silver). This pegging is what differentiates stablecoins from other cryptocurrencies, which are not backed by reserve assets and can greatly fluctuate.

Although there are various types of stablecoins, the most common types fall into the following three categories:

- Fiat-collateralized stablecoins in which the stablecoin is backed by a corresponding amount of fiat currency (e.g., USD or other traditional currency);
- Crypto-collateralized stablecoins in which the stablecoin is backed by other cryptocurrencies;
- Algorithmic stablecoins in which the stablecoin relies on complex algorithms to adjust supply based on market demand.

In addition to the reduced volatility that stablecoins offer, the use of stablecoins has several additional advantages, such as faster and cheaper cross-border transactions, access to financial services in regions with unstable currencies, easier access to the crypto ecosystem and freeze and seize functionality to combat illicit financing. However, the use of stablecoins is not without risk. The centralized reserve assets or entities still have their own underlying risk and could become compromised or mismanaged, there is regulatory uncertainty surrounding the use of stablecoins, and stablecoins may not offer the same level of privacy as some other cryptocurrencies.

Looking forward to 2025, due to stablecoins' transformative functionalities noted above, we expect the notion that "stablecoins" are simply a fad to disappear entirely and the adoption of real-world use cases to pick up momentum as 2025 progresses. In 2024, stablecoins already represented nearly a third of daily crypto usage, and we expect that to grow in 2025 as more and more commodity traders, producers, importers, shipping companies and other corporations will turn to stablecoins to solve certain business challenges related to fixing supply inefficiencies, speeding up global remittance flows, and resolving inefficient cross-border payment corridors between developed and underdeveloped markets.

CONTINUED ON PAGE 29

CONTINUED FROM PAGE 28

Cryptocurrency Mergers and Acquisitions in 2025 and Beyond

Stripe, a payment processing behemoth, recently acquired stablecoin platform Bridge for $1.1 billion. Bridge, which was founded in 2022, is an alternative payment method that allows businesses to store and accept stablecoins as payment and/or gives businesses the ability to issue their own unique stablecoin.

Stripe's acquisition of Bridge will likely have substantial impacts on the stablecoin market in the United States, such as:

- Lowering the cost of using stablecoins as a payment method, which will attract more businesses and consumers;
- Increasing competition in the stablecoin market, resulting in market pressure for other stablecoin-based companies to improve existing products or create new offerings;
- Creating the need for United States regulators to enact clearer guidelines around the use and acceptance of stablecoins as a payment method.

As noted above, we expect the use and acceptance of cryptocurrency to continue its U.S. growth in 2025 and beyond under the new, pro-crypto presidential administration, including a drastic increase in mergers and acquisitions in the stablecoin realm. This expectation is based on Trump's recent announcement that he intends to appoint Atkins chair of the SEC. Atkins is a strong proponent of cryptocurrencies and will likely play a key role in form-fitting regulation of the cryptocurrency industry and shaping key pro-business regulations that will support the growth of the cryptocurrency industry.

Privacy Rights Take Center Stage With Zero-Knowledge Proofs and Crypto Mixing

A zero-knowledge proof (ZKP) is a cryptographic technique that helps ensure privacy by enabling one party (the prover) to prove to another party (the verifier) that a value or statement is true without revealing any additional information apart from the fact that the specific value is true. For example, a ZKP can be used to prove a person is 18 without revealing the prover's identity or other unnecessary details. In a cryptocurrency context, ZKPs allow cryptocurrency users to make pseudonymous transactions on the blockchain while still retaining the ability to prove they meet certain eligibility requirements (like age, nationality or domicile) for those transactions.

Crypto mixing is a cryptographic technique that aims to obscure the transaction history of cryptocurrencies by combining various cryptocurrency users' coins into a pool and then redistributing the coins to new digital wallets, resulting in the enhancement of privacy for cryptocurrency users. Although there are obvious reasons to want financial privacy even over entirely legal transactions (would you want your bank account information to be publicly available?), crypto mixing is regularly associated with illegal activities due to the ability to use crypto mixing to conceal the source of illicit funds. The legality of crypto mixing varies by country and jurisdiction. In August 2022, the United States Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned digital asset mixing software "Tornado Cash" for the alleged use of the software by illicit actors in laundering more than $7 billion of virtual currency. Although the U.S. Court of Appeals for the 5th Circuit overturned the OFAC sanction on November 26, 2024, (based on the 5th Circuit's interpretation of federal law that OFAC overstepped its authority to regulate "property" by attempting to regulate crypto mixing, which does not constitute "property"), it is clear that the use of crypto mixing will continue to be aggressively monitored under both the current and next administrations.

In 2025, under the new administration, we expect the use of ZKPs to become more accepted in highly confidential industries such as health care and financial services, where highly sensitive electronic data is at stake and where ZKPs can make it harder for hackers to obtain that confidential information. We expect crypto mixing will continue to be under a closely watched microscope, as the benefits of financial privacy may be overshadowed by the ability of illicit actors to conceal funds through use of such technologies.

Private Industry Litigation Continues to Rise

In our 2024 predictions, we said that "a new wave of private litigation is occurring and likely to increase," which turned out to be correct. According to the Blockchain Association, the digital asset industry has spent over $430 million in litigation costs[2] in just actions brought by the SEC. While the change in leadership at the SEC is expected to dramatically reduce that administrative agency legal spend, at least some of those costs can be expected to shift to those incurred in private litigation.

[2] https://theblockchainassociation.org/regulation-by-enforcement/

CONTINUED ON PAGE 30

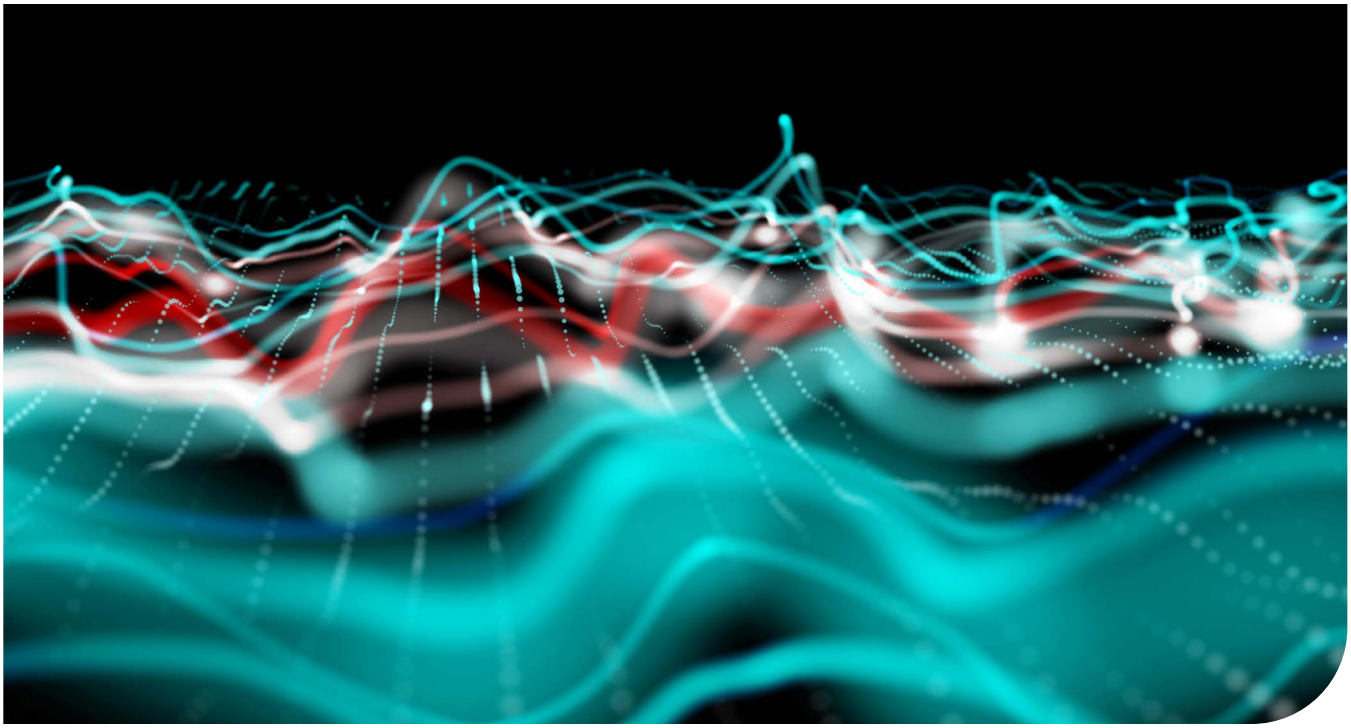
CONTINUED FROM PAGE 29

In the past year, there were class action lawsuits brought against NFT marketplaces and issuers, arguing those digital asset sales constituted unregistered securities transactions. There were bankruptcy-related actions regarding disputes dating back to the collapse of digital asset exchange FTX and related circumstances from 2022. Individuals brought lawsuits against decentralized autonomous organizations (DAOs), claiming participation in such organizations creates partnership liability for the actions of the DAO. These actions, and a host of other actions brought by individuals and entities regarding digital asset matters, demonstrate a rising trend of private litigation.

Industry participants should be prepared to address these litigation risks ahead of time with well-written agreements that properly account for the technical nuances of the underlying technology and through conscious decisions on legal structuring. While these lawsuits will primarily involve traditional contract, statutory and tort legal issues, which are not unique to digital assets, the knowledge of an attorney who is familiar with these assets and their unique features will be an essential factor in efficiently and successfully managing, addressing and resolving disputes involving blockchain-enabled products and services.

Conclusion

It is clear that 2024 marked a pivotal year for Web3, with unprecedented growth and transformative legal developments shaping the industry's trajectory. The anticipated regulatory shifts, burgeoning adoption of stablecoins, increased focus on privacy technologies like zero-knowledge proofs and a rise in private litigation are all signals of an evolving landscape. Companies exploring blockchain-enabled technologies and established players in the Web3 space must stay ahead of these trends to navigate the opportunities and challenges of 2025 effectively. With thoughtful legal frameworks, strategic planning and proactive compliance, the Web3 ecosystem is poised to continue its expansion, redefining how we think about digital assets, data ownership and the internet itself. Polsinelli's BitBlog Bi-Weekly will remain your go-to resource for tracking these critical developments in the year ahead.



AI for GCs: What You Need to Know in 2025

Reece Clark
Shareholder
Kansas City

Cat Kozlowski
Counsel
Los Angeles

Kelsey L. Brandes
Associate
Kansas City

Bryce H. Bailey
Associate
Dallas

During the course of 2024, interest in generative and other types of artificial intelligence, machine learning and predictive applications and services (collectively, AI) accelerated across industries. Some sectors, such as financial services, media and telecom, exceeded expectations for enterprise adoption. Others, such as life sciences, health care, energy and industrials lagged behind.[1] The largest obstacles to enterprise adoption have been appropriate scaling and identifying a return on investment (ROI). Those challenges will continue in 2025 and require a more critical examination by general counsels (GCs) and business leaders.

In our 2024 edition of AI for GCs: What You Need to Know, we identified certain AI adoption risks with a particular emphasis on user error and bias.[2] As 2024 played out, we observed these types of risks manifest through governance, public relations and regulatory issues for our clients. Yet even as companies focused on comprehensive solutions to mitigate these types of AI risks, other headwinds to AI adoption became apparent. Strategic, operational and compliance risks have coalesced to create a more complex adoption environment that is focused keenly on ROI.

As our 2025 edition discusses in more detail, GCs are now in a position to drive conversations beyond risk mitigation and legal compliance in AI tool selection. GCs will play a key role in shaping the conversations around opportunities and risks of AI adoption, and will find themselves continually asking the questions: What is the expected ROI of the AI tool, and how does that balance against legal risk?

Part 1: Empowering GCs to Diligence AI Solutions

In the nearly two years since the public reveal of ChatGPT 3.5, companies have experienced a roller coaster of reactions to the potential applications (and pitfalls) of "generative AI." Generative AI is a type of AI that individual users are more likely to directly observe as opposed to other types of AI that may recognize patterns or make predictions regarding data, transactions, images, or events, among other applications. Unlike generative AI, other types of AI have been in use for quite some time but have garnered less attention than generative AI. Retrospectively, the initial burst of excitement around the possibilities of AI (especially generative AI) was certain to moderate just as the picture of AI's usefulness would begin to come into focus. At the onset of the "gererative AI boom," some early movers invested in AI without a complete understanding of its current limitations and risks and have experienced challenges to implementation as a result.[3] Yet even as expectations around AI have begun to normalize, new AI solutions continue to launch at a breakneck pace. How then to make sense of the market?

Seasoned GCs know that over time, business leads become more discerning and realistic about the potential value a new technology can bring to the business. Shortly after a new technology launches, for example, excitement cools as the inflated expectations around its applications and capabilities fail to fully materialize.[4] AI is no exception. Moving into 2025, we expect businesses to continue recalibrating their views around AI and to further moderate their performance

[1] Brian Campbell et al., "Three ways generative AI can drive industry advantage," Deloitte (Oct. 30, 2024), https://www2.deloitte.com/us/en/insights/topics/strategy/artificial-intelligence-in-business.html
[2] Matt Todd et al., "AI for GCs: What You Need to Know for 2024," Polsinelli (Jan. 24, 2024), https://www.polsinelli.com/publications/ai-for-gcs-what-you-need-to-know-for-2024
[3] Eliud Lamboy, The AI Integration Challenge: Why Companies Struggle to Implement Artificial Intelligence, LinkedIn (July 20, 2024), https://www.linkedin.com/pulse/ai-integration-challenge-why-companies-struggle-lamboy-rn-mba-%CE%B4%CE%BC%CE%B4-neumc/
[4] Ankita Khilare et al., "Hype Cycle for Emerging Technologies, 2024," Gartner (Aug. 8, 2024), https://www.gartner.com/en/documents/5652523

CONTINUED ON PAGE 32

CONTINUED FROM PAGE 31

expectations. We expect this trend will be further accelerated due to more frequent instances of "AI washing" — a term GCs have (or will soon) become very familiar with.

AI washing occurs, for example, when vendors oversell the AI capabilities of their products, or mischaracterize routine data processes as being "powered by AI." From "robot lawyers" to bunk investment strategy tools, examples of AI washing increased during the back half of 2024 and will likely continue to pervade the market in 2025.[6] AI washing erodes trust in AI providers, risks regulatory enforcement from the Securities and Exchange Commission and Federal Trade Commission (FTC) and accelerates the pace of industry skepticism in AI capabilities and ROI.[7]

With this backdrop, GCs will experience a renewed sense of urgency to ensure proper diligence occurs on potential AI deployments. GCs should feel empowered, for example, to charge their business leads with gathering qualitative and quantitative information about potential AI deployments from both the business teams using the tool and the AI vendor. To create a complete cost-benefit view, GCs will want to consider, at a minimum, the following questions as their business leads are choosing AI tools:

- ***What data will the AI tool have access to?*** This is the most important question a GC faces. If the data profiles as low risk (e.g., historical budget information), then the overall risk from the AI tool is likewise lower. Conversely, if the AI tool will have access to personal information or sensitive business information, additional diligence is critical to ensuring the vendor has complied with applicable law, industry standard or better practices and rigorous security design in the development and maintenance of the AI tool.

- ***How was the AI tool trained?*** GCs should expect vendors to be able to produce a base level of information regarding how the AI tool, including the underlying data or model supporting such tool, were initially trained and validated and tuned and improved over time. To be clear, this is not asking a vendor to reveal trade secrets or sensitive proprietary information. Rather, a well-trained AI tool should be backed by high-quality and often proprietary datasets that are specifically targeted to the industry the tool is marketed toward. Be wary of AI vendors that have difficulty producing information about how their tool was trained or vendors that reveal their datasets were validated exclusively through open-source information (that often carry a broad "as-is" disclaimer and no representations of legality or quality). Where a vendor has used some open-sourced data, additional questions regarding infringement and privacy concerns are warranted. For example, ask whether the vendor can ensure all licenses and consents were procured from the parties or individuals who have supplied the underlying information which may include proprietary or personal information?

- ***How much risk does use of the AI present?*** Like any new field of technology, AI can present a variety of risks. There are strategic considerations evidenced by the need to scrutinize vendors for AI washing or overselling of their capabilities. Likewise, replacement of internal functionality with AI may bring a corresponding loss of human skill that needs to be carefully managed. There are compliance risks as well. These range from regulatory concerns to loss of company intellectual property (IP), security risks and ethical considerations. GCs will be particularly interested in how AI reduces operational challenges like recordkeeping, internal and external oversight and additional vendor/contract management. AI can also present new technology-based challenges, such as proper

[5] Bernard Marr, "Spotting AI Washing: How Companies Overhype Artificial Intelligence," Forbes (Apr. 25, 2024), https://www.forbes.com/sites/bernardmarr/2024/04/25/spotting-ai-washing-how-companies-overhype-artificial-intelligence/

[6] Kelly Miller et al., AI Washing Erodes Consumer and Investor Trust, Raises Legal Risk, U.S. Law Week (Oct. 25, 2024), https://news.bloomberglaw.com/us-law-week/ai-washing-erodes-consumer-and-investor-trust-raises-legal-risk. "Robot lawyer" company DoNotPay faces fines from the FTC for misleading customers that it could leverage AI to draft fully usable legal documents). Sheena Vasani, 'Robot lawyer' company faces $193,000 fine as part of FTC's AI crackdown, The Verge (Sept. 25, 2024), https://www.theverge.com/2024/9/25/24254405/federal-trade-commission-donotpay-robot-lawyers-artificial-intelligence-scams. Multiple investment firms have been implicated in lying about their ability to leverage AI and machine learning to improve their investment strategies. Press Release, U.S. Securities and Exchange Commission, SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence (Mar. 18, 2024), https://www.sec.gov/newsroom/press-releases/2024-36

[7] Marr, *supra* note 4.

CONTINUED ON PAGE 33

CONTINUED FROM PAGE 32

quality control for outputs and a clear user understanding of how to use the tools effectively. GCs should use extra scrutiny when leveraging AI in heavily regulated or mission critical areas as they consider risk profiles.

- ***What is the expected ROI?*** Consider the time horizon and total impact of the expected return and whether it is worth the initial capital investment. For example, will implementation of an AI tool cause a change in staffing? Efficiency gains from headcount reductions may be offset by transitional efforts and additional staffing for AI management, including output review, validation and legal or other compliance or quality reviews. Likewise, depending on the size and complexity of the implementation, the full project timeline may be quite long before seeing any payoff, and will that lengthy period justify the up-front cost? Use-case analyses can help outline the actual ROI and impact of a given service and set apart vendors offering real AI solutions from those merely AI washing their services. Finally, consider the risk from potential breakdowns in support that may come from a vendor leaving the market or tech becoming outdated, and how that change will be managed in a rapidly evolving market.

Part 2: Contracting With AI Vendors: Key Considerations

During the course of 2024, we saw a previous trend continue: the AI Addendum. These "one size fits all" attachments are designed to cover everything AI-related—and often suffer as a result from overly broad or underinclusive terms. Some examples of potentially problematic terms include requiring AI tools to be completely free of hallucinations and bias, meet multiple ISO and NIST standards, comply with data privacy and AI laws regardless of jurisdiction, disclose all training data and/or divulge all the model's secrets. When treating these addenda as "nonnegotiable" regardless of vendor agreement size or AI tool functionality, these fixed forms can create a disconnect between legal, the business and the AI tool's specific use case.

The better approach is for GCs to recognize AI and general-purpose models continue to change and, as a result, the contracting terms need to evolve with those changes. GCs should tailor and scale legal terms based on the applicable AI use case. For example, representations and warranties that a vendor will follow industry standards regarding data privacy and security, ethical use and governance will almost always be appropriate. Likewise, GCs may benefit from including transparency requirements, such as obligations on the vendor to maintain the necessary documentation to assist with regulatory inquiries or investigations in the event the vendor has or receives an adverse audit or complaint regarding the AI tool.

Other contracting considerations GCs should keep in mind:

- **Data Access Issues.** While vendors offering unpaid general-purpose models predominately seek rights to use company data as training data, the largest vendors provide a method for the user to opt out of training. For paid licenses, the prevailing approach from large language model (LLM) vendors continues to be for the user to own its inputs and outputs. For more negotiated downstream AI tool agreements, GCs may push to limit the vendor's use of company data to only that which is necessary to provide the contracted services or as separately agreed upon in writing. However, if the AI tool will have access to particularly sensitive data, GCs may want to also explore additional contractual pathways of protecting or further limiting use and access to the data, such as designating outputs as confidential information, restricting disclosure, explicitly prohibiting certain uses that may otherwise be assumed as a part of providing services (e.g. performance monitoring or debugging performed directly or through data aggregation), or limiting data retention.
- **Indemnification Considerations.** GCs should continue to take care in negotiating and reviewing the indemnification provisions in agreements for AI tools. If a tool has been trained or tuned on top of a general-purpose AI model, GCs need to identify whether they are protected from infringement and privacy claims regarding those materials. Depending on the use case, GCs may want to highlight other specific claims, such as bias or user-related errors and omissions. Similarly, GCs should watch out for caps and exceptions to liability, particularly for IP infringement, privacy or data breaches and violations of law. Generally, IP indemnification clauses include reasonable exceptions, such as if the user does not have proper rights to what they input, modifies the output, or intentionally attempts to cause the model to produce an infringing output. However, GCs should watch for additional

CONTINUED ON PAGE 34

CONTINUED FROM PAGE 33

conditions and requirements for indemnification, such as mandatory mitigation practices that require additional education or training for users.

- **Accuracy Requirements.** As a final risk mitigation consideration, GCs need to be aware that AI models, by design, are not stagnant. To prevent becoming "stale," models are regularly fed new training data that may fundamentally impact accuracy and performance and require more frequent corrective maintenance. A GC may therefore want to include minimums or additional explainability, transparency and reproducibility requirements. The more integral an AI tool will be for a company, the more precise performance and standards requirements should be, and the greater care GCs may need to dedicate to termination, vendor transition and operational contingencies should the tool or the vendor's business fail. GCs may also seek warranties that the AI tool will operate with reasonable accuracy for the nature of the use case, undergoes regular reviews and mitigation activities for data-based bias and is supported by a vendor team that will resolve reported errors.

Part 3: Looking Ahead to 2025: Balancing Risk and Reward

In 2024, GCs grappled with the business, legal and regulatory impacts of prospective AI implementations in their businesses. Seemingly overnight, GCs became a key figure in driving conversations regarding risk mitigation and legal compliance in AI tools and, in the process, rapidly developed new competencies in data archaeology, transparency, accessibility and privacy. In 2025, the combined effect of a more discerning environment for adoption of AI tools and the AI-related expertise GCs have gained means GCs will feature prominently in balancing risk and reward for prospective AI implementations and for developing a clear view of expected ROI.

As previously discussed, for some AI tools, the benefits take time to accrue, which means a company may not see a productivity return for several months or years. Now more than ever, it is key for GCs to consider ROI when analyzing AI tools to be used within the business.

When evaluating AI tools:

- Identify clear objectives that fit in with the company's goals and strategies;
- Document and monitor short-term and long-term outcomes including when outcomes transform from indirect to direct (and ask the vendor to provide evidence regarding the same);
- Ensure that the business has defined key performance indicators (KPIs) for use of AI tools and is actively monitoring such KPIs;
- Consider the total cost — including environment costs, implementation costs, training and tuning costs, and other maintenance, verification and staffing costs.

In 2025, we expect GCs will be challenging business owners more on AI tools, especially those that do not offer sufficiently clear ROI use cases to the business.

With government leaders taking office in several countries beginning in 2025, GCs will need to pay closer attention to current AI regulations and laws. Companies doing business in Europe, for example, will need to consider compliance with the EU AI Act. In the U.S., President-elect Trump has selected Sriram Krishnan, a former Andreessen Horowitz partner and entrepreneur, as the Senior Policy Advisor for Artificial Intelligence within the White House Office of Science and Technology Policy. This appointment signals a focus on maintaining U.S. leadership in AI innovation and a deeper focus on how AI interacts with various industries and digital infrastructure. U.S. states are also poised to continue passing a patchwork of their own AI laws and states with current AI laws (such as Colorado) may amend those laws to provide additional regulations. GCs will need to monitor both international and U.S. federal regulations and state laws applicable to their business to ensure compliance with such regulations and laws.

Conclusion

AI will continue to offer diverse opportunities to increase company efficiency and ROI when deployed strategically within the enterprise. As discussed, companies should ensure that the vendors they have selected understand the overall implementation strategy, especially at the point of initial discussions with the selected vendor. GCs should ask pointed questions about the project scope, resources needed and potential impact of the AI tool before a contract is executed and then continue to monitor the evolution of those impacts up to and after implementation. Properly scrutinizing various AI services will allow GCs and companies to evaluate the greatest ROI offerings and best vendor for a given implementation.

Trends in Negotiating With Software-as-a-Service Providers

Gregory L. Cohen
Shareholder
Phoenix

Scott M. Tobin
Associate
Chicago

Bryce H. Bailey
Associate
Dallas

Adam A. Garcia
Associate
Kansas City

Over the last two decades software-as-a-service (SaaS) has become the dominant form of software transaction. However, SaaS contracting forms and negotiating norms appear to be going through some potential changes, which we expect to accelerate in 2025 and beyond.

Before discussing the trends in SaaS transactions, however, it's important to understand the history and purpose of SaaS because that informs our understanding of future trends and the way that the law, business and technology around SaaS are evolving.

History of SaaS

SaaS contracting replaced and consolidated historically separate agreements for various elements of software typically installed and operated on the customer's premise and its computer systems and networks. These agreements often separately covered (i) software licensing terms, requirements, restrictions and pricing, (ii) software implementation and deployment terms and pricing, (iii) ongoing software maintenance and technical support terms and pricing and (iv) other provisions for hosting, governance and other matters. SaaS models generally consolidated the items above and replaced a perpetual license with a more limited periodic license and recurring periodic fees.

The widespread adoption of the SaaS model emerged alongside a broader market trend of subscription-based services. Several of the driving factors of SaaS adoption include the desire (i) by SaaS vendors to have recurring revenue, (ii) by SaaS customers for a single vendor to assume end-to-end responsibility for a software application and related infrastructure, (iii) by SaaS customers to reduce capital and other expenses related to computer hardware and infrastructure needed to operate software applications, and (iv) by both parties for greater financial certainty. A SaaS arrangement typically provides a more stable recurring and certain revenue stream for the SaaS vendor, while often providing the SaaS customer a bundled periodic subscription fee that may be easier for the customer to anticipate and budget.

SaaS Trends

SaaS vendors have long argued that multi-customer SaaS offerings necessitate using the vendor's form of contract, and in the earlier years of SaaS, few software customers had their own SaaS-specific forms. SaaS agreements continue to evolve, and the industry continues to gain experience in both the negotiation and outcomes of SaaS Agreements. Emerging regulatory concerns also increase the materiality of SaaS terms to businesses at large. As such, the following issues are increasingly subject to negotiation between the SaaS vendor and SaaS customer:

- **Form of Agreement:** There is often a significant disagreement between the SaaS vendor and SaaS customer as to which party's form of agreement to use. SaaS vendors will always want to use their own form of agreement while sophisticated SaaS customers often desire to use their own form of agreement.
- **Integration of other Forms:** In an effort to streamline both their SaaS agreement and negotiations, SaaS vendors often attempt to link to or refer to the SaaS vendor's standardized terms, policies, or procedures relating to various matters, including data privacy, security, subprocessors and other matters. From the SaaS vendor's perspective, this may discourage legal review and expedite or avoid negotiation cycles. From the SaaS customer's perspective, this introduces terms that may not have been fully reviewed or negotiated and which the SaaS vendor may be permitted to unilaterally modify in the future.
- **Privacy and Data Details:** The SaaS vendor and SaaS customer often enter negotiations having very different intentions and desires around the use of the customer's data that is processed and stored using the SaaS software. Customers often insist on more

CONTINUED ON PAGE 36

CONTINUED FROM PAGE 35

detailed and rigorous provisions around privacy compliance, data security and data use, including (i) approvals of or visibility into sub-processors/sub-contractors, (ii) where and how data is processed, (iii) mitigation and remedies for data incidents, (iv) maintaining certain industry specific qualifications, certifications, or standards (e.g., ISO, SOC II or III, NIST, etc.), (v) rights and/or limitations on de-identifying or aggregating data and (vi) rights and/or limitations on artificial intelligence (AI) training or tuning using customer data. Conversely, SaaS vendors often want increased rights to customer data for the vendor's own purposes along with greater flexibility in how and where it processes and maintains customer data.

- **Data Privacy Agreements:** SaaS vendors are becoming increasingly concerned that various foreign and domestic data privacy and security regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), now require the inclusion of data privacy agreements (DPAs) with their standard SaaS agreements. DPAs are standard alone agreements or schedules to the broader SaaS agreement that address the specific requirements of the GDPR, the CCPA, or other regulatory schemes. SaaS customers, especially those with purely domestic operations, often remain uncertain as to whether a DPA is truly required or is applicable to the customer's operations. The inclusion of DPAs with SaaS agreement, and whether it becomes prevalent across the software industry, is an emerging trend that we expect will come into greater focus in the upcoming year.
- **Data Liability Exposure:** As in many commercial agreements, vendors and customers often take contrary views regarding the vendor's maximum liability to the customer. In SaaS agreements, liability for issues and problems related the handling, processing, access and use of the customer's data is a central consideration. SaaS customers generally push vendors to assume risk and liability in excess of the annualized fees for privacy and data breaches (e.g., based on estimated potential exposure for the nature and volume of data involved, their cyber insurance deductibles, or other factors), either through an exclusion to the limitation of liability or an enhanced separate liability cap. SaaS vendors, however, typically try to limit their liability to annualized fees under the agreement or the vendor's insurance coverage (e.g., as may be required by the agreement with that customer or a percentage of its insurance considering the total exposure to all customers). SaaS negotiations often focus on the allocation of risk and liability, along with potential liability caps and exceptions to the liability caps, related to liability exposure for the misuse or unauthorized access to the customer's data.
- **Renewals and Price Increase:** The SaaS vendor and SaaS customer negotiations frequently focus on the renewal methods, potential price increases and growth in use of the software. While a SaaS vendor may seek the opportunity to grow the revenue associated with the SaaS agreement over time, a SaaS customer often seeks future cost predictability by attempting to restrain increases for additional use, during and after the initial subscription period, and for potential renewals after the initial subscription period. These discussions can be particularly challenging given the elevated macroeconomic inflationary pressures during the past several years.
- **Migration and Wind-Down Rights and Restrictions:** SaaS vendor and SaaS customer negotiations often include end of term data migration, wind-down and other rights, including the SaaS customer's rights to retrieve data and restrict post-expiration use of customer data for future AI or other purposes by the SaaS vendor.
- **Regulatory Issues:** Both SaaS vendors and SaaS customers are often concerned about future changes in privacy and data protection as they relate to the access, use and ownership of the customer's data including any future laws and regulations. As a result, both parties often seek to both future-proof the SaaS agreement and provide reasonable processes and guardrails to revise, re-price or terminate the agreement should changes in laws or regulations make that necessary.
- **AI:** SaaS vendors and SaaS customers are focused now more than ever on the potential use of customer data to broadly train and tune AI models. Vendors are seeking broad rights to use customer data to improve and develop future software products, including products that include AI components. Customers, however, are wary of allowing the broad use of their data for purposes unrelated to their business. The full scope of how a customer's data may be used in the future is unclear and likely to vary based on the software application, the customer's data and the industry.

CONTINUED ON PAGE 37

CONTINUED FROM PAGE 36

While many customers may wish to limit use of their data solely for the customer's own benefit, most SaaS vendors seek the ability to use the customer's data, often on a deidentified or anonymized basis, for a wider array of purposes.

- **Managed Customer Hosting.** Finally, and most interestingly, we are also occasionally seeing some vendors permit their customer to host and process (directly or with a third party cloud provider such as AWS, Microsoft Azure, or Google Cloud), all or some data within the customer's designated IT or cloud environment (as opposed to the vendor's owned or controlled environment), which is more like a pre-SaaS delivery on-premises license model. We expect this may become more prevalent in 2025 and beyond to address AI and data privacy and security concerns that both parties typically express. In some respects, this is also facilitated by the fact that vendors typically use one of these same third party cloud providers identified above as subcontractors and sub-processors in most SaaS models, so allowing the customer to engage and install directly in its own environment of a similar nature (i) does not necessarily create material inefficiencies from a support perspective, (ii) may decrease integration, throughput and latency issues associated with separate environments and (iii) gives the customer a sense of more control while letting the vendor distance itself from some risks and compliance issues.

Conclusion:

In conclusion, understanding and carefully negotiating SaaS contracting terms is crucial for both SaaS vendors and customers. Clear definitions of service scope, data security requirements and allocation of risk and liability can prevent future disputes and foster a successful business relationship between the parties. As SaaS continues to be the dominant software delivery model, conforming to best practices and identifying emerging trends will help organizations mitigate the risks and maximize the benefits of their SaaS arrangements.

About Our Technology Transactions & Data Privacy Practice

Polsinelli's Technology Transactions and Data Privacy team is comprised of over 70 lawyers with significant experience in the technology, privacy and cybersecurity industries.

We work with companies of all sizes and at all stages of development to provide strategic guidance as they create, acquire, use and commercialize technology. Our clients include businesses with domestic and international operations as well as governments, universities, hospitals, financial services institutions, startups and nonprofit organizations.

The Polsinelli team provides industry-leading data privacy counseling, incident response and breach litigation legal services. Our lawyers include former in-house data privacy attorneys, alumni of law enforcement agencies, attorneys with international backgrounds and some of the most experienced incident response lawyers in the country.

Contact one of our team members today to learn how we can help you and your organization with its technology, privacy and cybersecurity needs.

Stay Connected

Polsinelli frequently writes about topics related to these materials.

Click here to subscribe to receive news and webinar updates.

Editorial Board

Alexander S. Altman
aaltman@polsinelli.com

Bryce H. Bailey
bryce.bailey@polsinelli.com

Alexander D. Boyd
aboyd@polsinelli.com

Kelsey L. Brandes
kbrandes@polsinelli.com

Reece Clark
rclark@polsinelli.com

John C. Cleary
john.cleary@polsinelli.com

Gregory L. Cohen
gcohen@polsinelli.com

Starr Turner Drum
sdrum@polsinelli.com

Adam A. Garcia
agarcia@polsinelli.com

Sarah S. Glover
sglover@polsinelli.com

Xeris E. Gregory
xgregory@polsinelli.com

Adam Griffin
agriffin@polsinelli.com

Ephraim T. Hintz
ehintz@polsinelli.com

Courtney P. Klaus
cklaus@polsinelli.com

Sara Kopetman
skopetman@polsinelli.com

Cat Kozlowski
ckozlowski@polsinelli.com

Greg M. Kratofil, Jr.
gkratofil@polsinelli.com

Noor K. Kalkat
nkalkat@polsinelli.com

Gregory J. Leighton
gleighton@polsinelli.com

Shundra Crumpton Manning
scmanning@polsinelli.com

Romaine C. Marshall
rmarshall@polsinelli.com

Mark A. Olthoff
molthoff@polsinelli.com

Todd Panciera, Jr.
tpanciera@polsinelli.com

Jessica L. Peel
jpeel@polsinelli.com

Mary Ann H. Quinn
mquinn@polsinelli.com

Anna K. Schall
aschall@polsinelli.com

Jonathan E. Schmalfeld
jschmalfeld@polsinelli.com

Elizabeth Snyder
esnyder@polsinelli.com

Pavel (Pasha) A. Sternberg
psternberg@polsinelli.com

Scott M. Tobin
scott.tobin@polsinelli.com

Eric S. Wu
ewu@polsinelli.com

POLSINELLI | What a law firm *should* be.™