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

JANUARY 2024

2024 REPORT

Technology Transactions & Data Privacy

As we start 2024, it is essential to consider the impactful progress in technology, privacy and data security that characterized the past year, while also looking forward to the ever-expanding future. Our fourth annual Technology Transactions & Data Privacy Report delves into the dynamic landscape of incident response, privacy litigation and the day-to-day dealings around data counseling and contracting.

From groundbreaking court decisions to emerging trends, our report provides a comprehensive overview of the legal issues that defined last year. We also offer insights into data privacy best practices and provide guidance for organizations navigating the intricate web of personal information protection. In an era where data is the new currency, understanding and implementing robust privacy measures is more crucial than ever. From cyber insurance and vendor management strategies to compliance frameworks, our report aims to equip readers with the knowledge to safeguard sensitive information effectively.

Looking ahead, the intersection of artificial intelligence ("AI") and data privacy will become a focal point in a number of areas. My introduction last year was written shortly after the launch of ChatGPT and represented my first professional use of generative AI. It is now a regular part of my personal and professional life. We believe 2024 will be defined by the ethical considerations, regulatory frameworks, landmark court cases and the evolving landscape of AI. Polsinelli attorneys will continue to be at the forefront of AI.

We are often called upon to address novel issues during an organization's most vulnerable time. Our attorneys are passionate about cybersecurity and data privacy and recognize the role we play in shaping and safeguarding our client's businesses today.

Sincerely,

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

Table of Contents

Arbitration Of A Data Breach Lawsuit: Defeating Class Actions With Arbitration Clauses And Class Waivers

Mark A. Olthoff
Shareholder
Kansas City

Courtney P. Klaus
Associate
Kansas City

The number of data breach class actions has surged in recent years, and this trend shows no signs of slowing down. In 2022, an average of thirty-three data breach class actions were filed in federal court every month. In June of 2023 alone, over sixty were filed. Are there alternatives to fighting battles in open, public courts? Are there options to potentially reduce the costs of litigation in lawsuits?

Arbitration clauses and class action waivers can be a possible solution. This article discusses how arbitration clauses have been used in data breach cases and whether they might be considerations in the future.

Benefits of Arbitration Clauses

Arbitration can be an effective way to avoid the expensive delays of litigation in court. Larger organizations often prefer arbitration because it bypasses lengthy hearing processes, keeps litigation confidential, and gives the parties a say on who becomes the ultimate decisionmaker. Arbitration clauses may also include class action waivers, which can prevent large groups of people from consolidating their claims. These benefits of arbitration, accompanied by class action waivers, are especially attractive to companies seeking to mitigate the costs of data breach litigation, where organizations may face huge class sizes and significant reputational damage.

Arbitration and Class Waiver Success in Recent Data Privacy Cases

Recently, a district court in Maryland certified classes of over a hundred million people following a data breach involving a customer loyalty program. The defendants soon after appealed the certification rulings. In October 2023, the Fourth Circuit vacated the certification decisions, ruling that the district court must evaluate the existence of a class waiver before a class action can proceed. The presence of an arbitration clause or class action waiver is to be considered at the initial stages of a case. In other words, a class action waiver is not a defense to liability but a defense to being required to litigate a class action at all. Upon remand, the district court reinstated the class certification orders. The court found that the class action waiver provisions had been waived because the defendant failed to advance the waiver arguments and, instead, agreed to multidistrict litigation in a single court, which it observed was inconsistent with class action waiver.

In another case, the Northern District of California found that the representative plaintiff in a data breach lawsuit had agreed to an online dating service's terms of use which contained a class action waiver. The court then denied the plaintiff's motion for class certification. Similarly, an e-commerce website convinced the Sixth Circuit to dismiss a class action and compel arbitration where its amended terms of service included an arbitration provision. And in another case, a video gamer was prevented from bringing a class action lawsuit because the end user license agreement the plaintiff signed included an arbitration clause.

CONTINUED ON PAGE 3 ▸

CONTINUED FROM PAGE 2

As these cases show, arbitration clauses and class action waivers can provide significant relief to avoid costly lawsuits. While not every interaction with a company may create an opportunity to include arbitration and class action waiver agreements, such instances do exist where companies enter transactions. For example, arbitration clauses are common in employment agreements and consumer-facing agreements. As mentioned above, terms of service and licensing agreements may include them as well.

Keeping Arbitration Clauses Enforceable

Not all arbitration clauses and class action waivers are enforceable. Mistakes and blind spots increase the risk that a company will be forced to litigate against a class action lawsuit it attempted to avoid with a waiver. Below is a list of steps an organization can take to prepare itself for an enforceability challenge to arbitration provisions in court.

1. **Provide Proper Notice.** When a standard form agreement includes an arbitration clause, courts often look to consent between parties to decide whether the agreement should be enforceable. Courts have found that a plaintiff consents to new or updated arbitration agreements when companies provide conspicuous notice of updates to terms of service. However, imprecise language that fails to clearly explain a consumer's rights does not provide the consumer with proper notice that they have entered an arbitration agreement. Furthermore, while some courts have found that silence from a consumer is enough to prove consent, other courts, like the Supreme Court of Indiana, require a more substantial showing of consent from the consumer, particularly where agreements are amended and the amendment is to be effective unless rejected by the party. Companies may avoid these consent-related problems by issuing notices that clearly describe a consumer's rights and by requiring an affirmative act on the part of the consumer, like clicking an "accept" button to new terms.
2. **Do Not Waive the Arbitration Right or Class Waiver.** Whether or not a party has a valid arbitration clause, the party can inadvertently waive the right to arbitrate in litigation. The same is true of class waivers. A party waives its arbitration right or class action waiver if it has knowledge of the right and acts inconsistently with that right. Acting inconsistently with an arbitration right includes litigating on the merits without raising the arbitration right first. In a recent Ninth Circuit case, the court found the defendant could not compel arbitration of absent class members' claims after it had already substantively challenged a representative plaintiff's claims over the course of six years. In another case in the same court, the defendant had not waived its arbitration right when it pleaded arbitration as an affirmative defense in its answers to the plaintiff's original and amended complaints. In a recent District of Maryland case, the court found a defendant had waived its argument to force individual actions by, among other things, agreeing to consolidate the action in a jurisdiction different from the waiver's accompanying choice of law provision. This case is a reminder that it is important to consider the full language of an arbitration clause or class waiver provision to ensure that a party does not inadvertently take steps that could invalidate it.
3. **Consider a Jurisdiction's Public Policy.** While arbitration agreements are generally enforceable under the Federal Arbitration Act, courts sometimes will strike down arbitration clauses or class action waivers if the court finds the agreements are unconscionable or contrary to public policy objectives. Public policy objectives are evidenced by laws that explicitly provide for class action rights. For example, this year the District of Rhode Island held that a class action waiver was not enforceable when a plaintiff brought an action under the Rhode Island Deceptive Trade Practices Act. In that case, the waiver ran contrary to Rhode Island's public policy objectives.
4. **Review and Revise.** If an agreement already exists without an arbitration clause or a class action waiver, a company might consider amending the agreement to add one. Courts have typically held that companies can add new arbitration clauses to already existing agreements, provided they meet certain notice requirements. It is important to stay abreast of what the jurisdictional requirements are for arbitration agreements and what the court says about public policy in the state.

Risks and "Mass Arbitration" Developments

The rise of arbitration clauses and their prevalence in the class action space is not without controversy or risk. Activist groups have criticized the prevalence of arbitration clauses and class action waivers as a sort of "get-out-of-jail-free card" that impedes the defense of an individual's right to privacy. And, in a world of "be careful what you ask for," sometimes enforcing class waivers in arbitration can be costly as well.

When a book rental website experienced a data breach, a law firm seeking to exploit an arbitration provision filed 15,107 individual arbitration demands. This "mass arbitration" can be costly for companies that promise in their agreements to bear certain arbitration costs, such as filing fees. In that case, $300 individual filing fees would add up to approximately $4.7 million when all the demands were totaled together. In another case, currently in the Seventh Circuit, a company is appealing a district court's order that would require it to pay about $4 million in arbitration fees in connection with roughly 35,000 individual arbitration demands.

Current Issues In Data Breach Class Action Settlements

Mark A. Olthoff
Shareholder
Kansas City

Shundra Crumpton Manning
Associate
Nashville

Very few civil cases ever reach a jury. Nearly every lawsuit is at some point resolved by the court on motion or through settlement. Class action cases are no different, including those filed after data breach incidents. Accordingly, developing a strategy early in a lawsuit timeline is critical – whether to seek an early dismissal or an early out of court resolution. This article discusses a number of developments in the past year impacting class action settlements. And whether a case settles for tens of millions of dollars or substantially less, these recent events should be a part of any settlement consideration.

Class Certification

First, as we reported last year in this publication, two federal courts recently certified classes in data breach cases. Both cases were appealed and, in each instance, the appeals courts reversed or vacated the district court decisions (albeit for different reasons). While the lower courts' certification orders demonstrate data breach cases can be appropriate for class treatment, the fact that appeals courts have closely scrutinized the district courts' conclusions also shows there is uncertainty. In turn, a well-known axiom for any settle environment is where uncertainty exists on either or both sides.

Claims Rates and Notices

Second, courts, particularly in the federal system, are increasingly scrutinizing settlements in terms of fairness, reasonableness, and result. Courts are evaluating the claim rates and adequacy of notices being used. A California federal judge recently complained that predicted rates of 1%-9% were too low. He also found that the settlement notice provided to class members was too long and complicated. In denying the plaintiffs' motion for preliminary approval, the judge told the lawyers to find a way to boost up the expected number of claims. In another recent instance, a Michigan federal judge became irked when the settlement presented to him describing potential payouts failed to consider that settlement costs and attorney fees were being deducted from the settlement fund. He found the notice was misleading and rejected preliminary approval. The First Circuit Court of Appeals also recently vacated a class settlement where it found significant differences in the claims created conflicts within the class requiring separate class representatives and would not allow for equal treatment of class awards. Finally, the Second Circuit Court of Appeals vacated a settlement finding there is no "presumption of fairness" as to a settlement agreement that was negotiated at arm's length during a lengthy mediation before a neutral party. Rather, district courts must fully analyze all aspects of a settlement under the factors in Rule 23.

Aggregators and Artificial Intelligence

Relatedly, another somewhat recent development is the introduction of third-party aggregators using artificial intelligence ("AI") to boost objection, opt-out, and claims rates. In essence, aggregators are using AI to locate class members and then communicate with them to file objections, opt-outs (with the possibility of filing other suits), or submit claims on behalf of the class members. At least one court has sounded an alarm and rejected the use of an AI aggregator for these purposes. *See In re Juul Labs, Inc. Marketing, Sales Practices, and Products Liability Litigation,* 2023 WL 6205473 (N.D. Cal. Sept. 19, 2023). The court overruled objections and set aside aggregated claims reasoning there was a lack of control over class communications and notice. On the other hand, some commentators have expressed that the use of AI could lead to more class member participation, better class notice, improvements in class administration, and higher claim rates. That said, AI is not a panacea for all problems and safeguards to prevent abuses and fraud would have to be implemented.

Attorney's Fees

Counsel fees continue to be a source of judicial consternation and a number of courts have continued to question attorney's fee awards in settlements. In a June 2023 Ninth Circuit Court of Appeals opinion, the court reversed (and revoked) a district court order where the plaintiffs initially sought $6 million and the court reduced it to $1.7 million. Still, the appeals court rejected the amount because – in the claims-made settlement – only $53,000 in compensation was claimed. This resulted in attorney's fees of more than 30 times the amount. This case and others like it are now being used to change class action settlement structures. Plaintiffs are aggressively pushing for settlement terms that include non-monetary class-wide relief such as credit monitoring or certain forms of injunctive relief to demonstrate the value of the class settlement. There are also a significant number of cases where plaintiffs are demanding a common fund structure (as opposed to claims-made) to reduce the risk that settlements are not approved because they do not sufficiently compensate class members. Historically, claims-made settlements have been a better approach in data breach settlements because the structure permits compensation to be awarded to those class members that have interest in the settlement and have been harmed by the incident. A common fund structure, on the other hand, merely distributes a settlement fund without regard to anyone's possible damage – potentially resulting in overpayments and underpayments to particular class members.

CONTINUED ON PAGE 5 ▸

CONTINUED FROM PAGE 4

Residual Settlement Funds

Finally, residual settlement funds have received attention in the past year. Frequently, in a common fund settlement, these are funds remaining due to an inability to locate every class member. Several alternatives exist to distribute the remainder: (1) reversion to the defendant, (2) re-distribute to the class members who are known, (3) distribute to a *cy pres* recipient, (4) or escheat to a government. Ordinarily, courts reject returning money to the defendant that paid to settle and, in some instances, it is infeasible or uneconomical to re-distribute to the class members. This leaves alternatives (3) or (4) most likely. In the past year, courts have continued to struggle with the tension of distributing money to a *cy pres* recipient that has no connection to the lawsuit and judges determining how much should be awarded to any particular organization. In addition, critics have commented that *cy pres* awards divert funds from the real beneficiaries of the settlement. This said, courts have recently approved both *cy pres* distributions and awarded residual funds to the U.S. Treasury. The validity and application of *cy pres* and other alternatives will continue to be addressed by the courts.

Each of these developments will continue to impact the future of data breach class actions and settlements. There are opportunities to be creative and seek novel ways to resolve these claims and parties and counsel alike should be open to building settlements that can reach the proposed classes yet also consider the necessary safeguards to protect against abuses.

The VPPA (Video Privacy Protection Act) Class Action – Is this Tide Still Coming in? Or Going Out?

John C. Cleary
Shareholder
New York

Jonathan E. Schmalfeld
Associate
St. Louis

The Video Privacy Protection Act (VPPA)[i] had quite a year in 2023. Building on its newfound stardom and cachet in the hands of the plaintiff class action bar toward the end of 2022, the VPPA just kept growing and growing in early 2023. Case filings were up (in federal and state court). Sectors targeted for litigation kept expanding – from traditional video purveyors to banking, sports, manufacturing, health care, print media and websites with embedded videos accessible for viewing and downloading.

However, by the end of 2023, the tide began to turn against VPPA plaintiffs, with previously agreed settlements subjected to criticism by the courts and defendants obtaining early dismissals on constitutional and statutory grounds. This article will take stock of the turbulence engulfing the VPPA class action lawsuit trend and offer a path forward for companies in search of best practices and the most effective defense strategies headed into 2024.

Background on VPPA

The VPPA was enacted in 1988 following an incident where a video store clerk disclosed Judge Robert Bork's video rental records, which were subsequently publicized in the media during his hearing for confirmation to the Supreme Court. Amid public surprise and concern from across the political spectrum, Congress amended the federal code to prohibit, with certain exceptions, the disclosure of video rental records containing personally identifiable information.[ii]

While the VPPA was initially intended to prevent video rental companies from sharing details regarding those rentals, creative plaintiffs' attorneys started using the VPPA for liability claims against streaming companies with the rise of online video streaming in the early 2000s. This has helped shape much of the case law regarding applicability of the VPPA to streaming video tracking.[iii]

The term "consumer" is defined in the VPPA as "any renter, purchaser, or subscriber of goods or services from a video tape service provider." The case law is split on exactly what makes someone a "subscriber" so as to meet the definition of "consumer" under the VPPA.[iv] Generally, subscribing involves some type of commitment, relationship, or association (financial or otherwise) between a person and an entity but does not necessarily require payment.

In 2022, there was a sharp increase in litigation under the VPPA against websites which had videos available for viewing on their sites which was often coupled with Facebook Pixel/Meta Pixel tracking on

[i] 18 U.S.C. § 2710

[ii] The VPPA permits disclosure of such information: (1) to the consumer; (2) with the written consent of the consumer; (3) pursuant to a federal criminal warrant, an equivalent State warrant, a grand jury subpoena, or a court order under specified guidelines; (4) to any person if such disclosure is solely the names and addresses of consumers and the consumer has had the opportunity to prohibit such disclosure; (5) to any person if such disclosure is incident to the ordinary course of business of the video tape service provider; or (6) pursuant to a civil court order.

[iii] *See In re Hulu Privacy Litigation*, No. C 11-03764 LB, 2012 WL 3282960, at *6 (N.D. Cal. Aug. 10, 2012); See In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262, 290 (3d. Cir. 2016) ("companies in the business of streaming digital video are well advised to think carefully about customer notice and consent.").

[iv] *See Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251, 1255–58 (11th Cir. 2015) ("Subscriptions involve some or [most] of the following [factors]: payment, registration, commitment, delivery, [expressed association,] and/or access to restricted content." (alterations in original) (citation omitted)).

CONTINUED ON PAGE 6

CONTINUED FROM PAGE 5

the website. At the time, the case law was unclear whether individuals browsing website videos are "subscribers" under the VPPA or if merely putting videos on a website makes the website operator a "video tape service provider" subject to potential VPPA liability.

VPPA Case Developments in 2023

One of the first heavily publicized cases in this new wave of VPPA cases was against Boston Globe in early 2022.[v] The lawsuit alleged the Boston Globe's integration of the Meta pixel tracking functionality onto sections of their website which were only available to Boston Globe subscribers violated the VPPA to the extent that tracking included tracking integrated video views on the website. In the year following the filing of the Boston Globe lawsuit, over 100 class actions were brought against online news outlets, streaming services retailers and others, almost all of which were based on use of the Meta pixel on those websites.

After fiercely litigating the case for over a year, the Boston Globe eventually reached a $5 million settlement. However, subsequent to the settlement, U.S. District Judge Richard Stearns dramatically reduced an agreed $1.7 million in plaintiffs' attorneys' fees down to $750,000.

According to Bloomberg, as of November 2023 of those over 100 cases, 17 had been dismissed by the courts, 29 were voluntarily dismissed by plaintiffs, potentially as a result of private settlements, and only 19 resulted in class-wide settlements or other public settlements.[vi] The dismissals by court order were led by courts largely agreeing that subscription to a website's newsletter which may have video content is not sufficient to make an individual a "consumer" under the VPPA.[vii]

In addition to the above examples of attorneys' fees being criticized and reduced in settlements of VPPA cases and dismissals being achieved by defendants by motion, the slowdown in this wave of litigation may also be a result of targeted websites and companies adding compliance plans and reconfiguring their business practices. Additionally, given some of the criticism by courts and commentators, it is perhaps inevitable that Congress and key regulators may start to take renewed interest in how such an ancient, single-purpose pre-internet law could be so dramatically weaponized in 2022 and 2023 as a vehicle to attack and "regulate" e-commerce and routine data analytics.

Also relevant is the newly crowded field of other statutory damage claims under federal and state laws, particularly the California Invasion of Privacy Act and the federal Electronic Communications Privacy Act, as discussed elsewhere in this Tech Transactions & Data Privacy Report: 2024. It remains to be seen if these potentially "greener pastures" will draw attention and energy away from new VPPA class action suits.

Best-Practices Moving Forward in 2024

While the more dubious stretches of the VPPA statutory language have tapered off somewhat in newly filed suits, there are still cases being regularly brought against websites which have third-party video tracking services behind subscription login pages.

Going forward, websites that wish to put videos behind a log-in section and track the viewership of those videos through any third-party service should institute a policy of obtaining regular express user consent to such tracking. This is an emerging best practice even if no payment is involved and users merely need to create accounts to have access to those sections of the website.

Companies should also assess their uses of tracking on web pages with integrated video features. Some general good practices include removing all embedded videos from websites and instead redirecting individuals to third-party websites such as Instagram or YouTube to view, configuring website plug-ins (including the Meta pixel) to disable "Content View" or "Page View" function either sitewide or on any landing page with a video, or requiring affirmative acknowledgment by users that they understand the website's tracking functions apply to videos the users view before a user is permitted to view any embedded video on a company's website.

End Thoughts

The journey of the VPPA through 2023 has been quite a roller coaster, marked by a significant rise in class action lawsuits followed by a notable shift in the legal landscape toward the end of the year. This shift saw a reduction in settlements and an increase in early dismissals, signaling a potential decline in the VPPA's role in litigation on a class-wide basis against key sectors and types of websites.

The year's developments highlight the evolving nature of privacy law and its application in the digital age, especially concerning video content and tracking. For companies, this underscores the importance of staying abreast of legal interpretations and adapting their practices accordingly. Instituting policies like obtaining express user consent for video tracking, reassessing the use of embedded videos and reconfiguring website tracking functions is now essential.

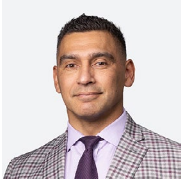
As we move into 2024, it is clear that the landscape of privacy law, especially in relation to the VPPA, remains dynamic. Companies must continue to navigate these changes proactively, ensuring compliance and reducing litigation risks in an increasingly digital world.

[v] *Ambrose v. Boston Globe Media Partners LLC*, 1:22-cv-10195 (D. Mass. Feb. 5, 2022).

[vi] Witley, Skye, *Video Privacy Class Action Wave Slowed by High Dismissal Rate*, Bloomberg Law https://news.bloomberglaw.com/privacy-and-data-security/video-privacy-class-action-wave-slowed-by-high-dismissal-rate

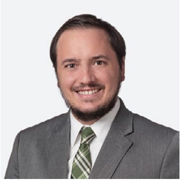
[vii] *See, e.g., Salazar v. Paramount Global,* 3:22-cv-00756, Dkt. #33 (M.D. Tenn. July 17, 2023); *Carroll v. The J.M. Smucker Company et al,* Case No. 3:22-cv-08952, Dkt. #36 (N.D. Cal. June 15, 2023).

Considerations for Artificial Intelligence and Employment Law

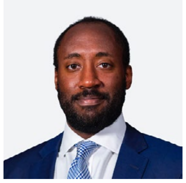


Romaine C. Marshall
Shareholder
Salt Lake City

Jason N.W. Plowman
Employment Class & Collective Actions Co-Chair
Salt Lake City



Matthew P.F. Linnabary
Associate
Kansas City



Aaron A. Ogunro
Associate
Chicago

Considerations for Artificial Intelligence and Employment Law

As artificial intelligence ("AI") technologies become more ubiquitous and advanced, both the advantages and potential risks they pose for employers continue to grow as well. This is especially true with regard to the use of generative AI – that is, AI that can generate original content based on data patterns. This type of AI can produce original images, text, music and designs, among other things. With the rising use of AI, we are seeing a corresponding rise in legislation, guidance and litigation addressing the use and consequences of AI. One area where this is increasingly common is the employment sphere.

AI in the Employment Cycle

More and more, employers are using AI in various aspects of the employment cycle. Recruitment is one of the stages when AI is used most, including through resume screening, video interviews, pre-employment assessment and automated candidate services. During employment, AI may be used in various ways, such as automated employee service, skill development, performance management and in various everyday work tasks.

These usages, though, can pose various risks to employers that use AI.

The Risks of AI in Employment

Title VII and Machine Learning AI

Title VII – the landmark anti-discrimination law – prohibits employers from using neutral tests or selection procedures unrelated to the position and inconsistent with business necessity when those tests or procedures disproportionately exclude persons of a protected class (i.e., race, color, religion, sex, national origin).

When such an effect results from such neutral tests or selection procedures, it is known as disparate impact or adverse impact discrimination. This type of discrimination is generally only an issue with predictive AI tools because that type of AI utilizes algorithms to recognize data patterns and make predictions – which can lead to biased results when the underlying algorithms are biased (even if inadvertently so).

In May 2023, the Equal Employment Opportunity Commission ("EEOC") released guidance specifically addressing the use of AI for employee selection processes. According to the EEOC, AI has an "adverse impact" when the selection rate for one group is "substantially" less than the selection rate for another group. The May 2023 guidance set forth the "Four-Fifths Rule" for determining what "substantially" means. The acceptance rate for a class of applicants is "substantially" different from the acceptance rate of another class of applicants if the ratio of the two rates is less than four-fifths (80%). Not only do employers need to make sure their selection processes are in line with these requirements, but they can still be liable for discriminatory selection procedures even if the AI tool used for the procedures was developed by a third party or administered by an agent.

ADA and Machine Learning AI

Similar to what was done with Title VII, the EEOC issued guidance addressing concerns with the use of AI in interacting with the requirements of the Americans with Disabilities Act ("ADA"). That guidance provides three main examples of AI violating the ADA:

1. If the AI usage results in a failure to provide a reasonable accommodation – this may occur when an applicant or employee requests a reasonable accommodation and the disability is likely to make it more difficult to use the AI tool or make an assessment less accurate and the employer fails to provide an alternative format.
2. If the AI usage results in an intentional or unintentional screening out of disabled applicants – this may occur when an AI tool results in lower scores for assessments as a result of a disability, such as giving a lower rank to applicants with significant gaps in employment history or with specific speech or movement patterns.
3. If the AI system makes "disability-related inquiries" or conducts "medical examinations" prior to extending a conditional offer of employment – this can also violate the Genetic Information Nondiscrimination Act.

CONTINUED ON PAGE 8 ▸

◂ CONTINUED FROM PAGE 7

Labor Law and AI

The broad scope of Section 7 of the National Labor Relations Act's right of employees to self-organize and bargain collectively can also be affected by AI usage. The National Labor Relations Board General Counsel issued a memo in October 2022 setting forth numerous ways the use of AI tools can violate Section 7, including when:

- AI tools surveil/gather information regarding employee Section 7 activities – even if merely creating the impression of surveillance;
- Employees are disciplined for protesting the use of AI tools for employee monitoring/management;
- AI tools include personality tests to evaluate an employee's propensity to engage in protected Section 7 activities;
- AI tools use algorithms to make decisions based on union representation;
- AI tools use algorithms that include production quotas or efficiency standards to single out union supporters;
- Employers fail to provide information about the implementation/use of AI technology to employees; and
- Employers fail to bargain with employees over the implementation/use of AI technology in the workplace.

Legislative and Litigation Trends

Cybersecurity

Adding to the growing mix of guidance is November's *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (EO).[i] Among other things, the EO addresses cybersecurity requirements that must be considered by federal agencies and AI developers given AI's ability to be leveraged by threat actors.

Cybersecurity threats posed by AI – known as, *adversarial* AI – include the vivid examples highlighted by Jonathan Care in his article aptly titled, "Fight AI with AI."

> [A]n autonomous vehicle that has been manipulated could cause a serious accident, or a facial recognition system that has been attacked could misidentify individuals and lead to false arrests. These attacks can come from a variety of sources, including malicious actors, and could be used to spread disinformation, conduct cyberattacks, or commit other types of crimes.

For these and other safety and security reasons, the EO requires the establishment of an advanced cybersecurity program to develop AI tools to find and fix vulnerabilities in critical software. The EO also includes deadlines by when certain standards must be established for such things as physical and cybersecurity protections (90 days) and safety and security guidelines for use by critical infrastructure owners and operators (180 days).[ii]

Data Privacy

Another major concern with AI is its natural intersection with data privacy – AI usage of consumer and employee data lends itself to potential problems with maintaining the privacy of that data. At the same time, many states are taking a stronger approach to data privacy, with numerous states passing data privacy laws in the past year or so, with some of those states – including California, Colorado, Connecticut, Iowa, Utah and Virginia – even specifically addressing AI in their privacy laws.

Beyond just state law, the Federal Trade Commission ("FTC") has also exercised its authority to regulate algorithmic consumer data usage under Section 5 of the FTC Act, Fair Credit Reporting Act and the Equal Credit Opportunity Act. The FTC specifically has encouraged deployers of AI to take steps to:

- Ensure transparency through disclosures;
- Monitor data inputs and outputs to prevent class discrimination;
- Grant user-access to delete or correct personal information;
- Ensure output data is accurate;
- Protect the algorithm from unauthorized use or breaches;
- Implement accountability structure to help maintain compliance.

The FTC further recommends that employers remove any identifying data before entering it into any AI platform.

Data privacy concerns in particular are becoming a heightened concern for employers, as courts begin to view employer obligations in protecting such data more broadly. In *Ramirez v. Paradies*, the Eleventh Circuit found that traditional tort law – and the duty of care, the special relationship between employers and employees, and the foreseeability of harm thereunder – could impute liability to an employer that suffered a ransomware attack on its administrative systems leading to the unauthorized disclosure of current and former employees' social security numbers. With AI potentially increasing the collection of personal information on employees and courts and legislatures heightening scrutiny on employer protection of that information, employers should take a careful look at their processes and procedures for protecting employee data.

Automated Employment Decisions

New York City has already passed a law regulating automated employment decision tools ("AEDTs"). The law is meant to prevent bias in the use of AEDTs and requires that AEDTs undergo bias auditing within the year prior to use when (a) the employer relies "solely" on the AEDT in making employment decisions; (b) the employer relies on other factors in addition to the AEDT output but weighs the AEDT output more heavily than any other criterion; or (c) the AEDT output is used in a way that can overrule conclusions from other factors, including human decision-making. In addition to the bias auditing, employers must also provide notice to employees and applicants of the AEDTs' use and publish the audit results, and they must retain AEDT records and reveal them to employees upon request. As the use of AI and

[i] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/
[ii] Id. at §§ 4.2(c), and 4.3(a).

CONTINUED ON PAGE 9 ▸

◂ CONTINUED FROM PAGE 8

AEDTs increases, an increase in this type of regulation can be expected.

Under the draft regulations, ADMT has a broad definition and includes any system, software or process (including those derived from AI) that processes personal information and uses computation, either on its own or as part of a system, to make or execute a decision or facilitate human decision-making.

Specific AI State Legislation

Many state legislatures, including those of California, Massachusetts, New Jersey and Vermont, as well as the D.C. legislature, have proposed legislation relating to the use of AI in the employment sphere. More states will likely follow suit. These laws would be expected to prohibit "algorithmic discrimination" and put in place notice and accommodation requirements for the use of AI in employment decisions.

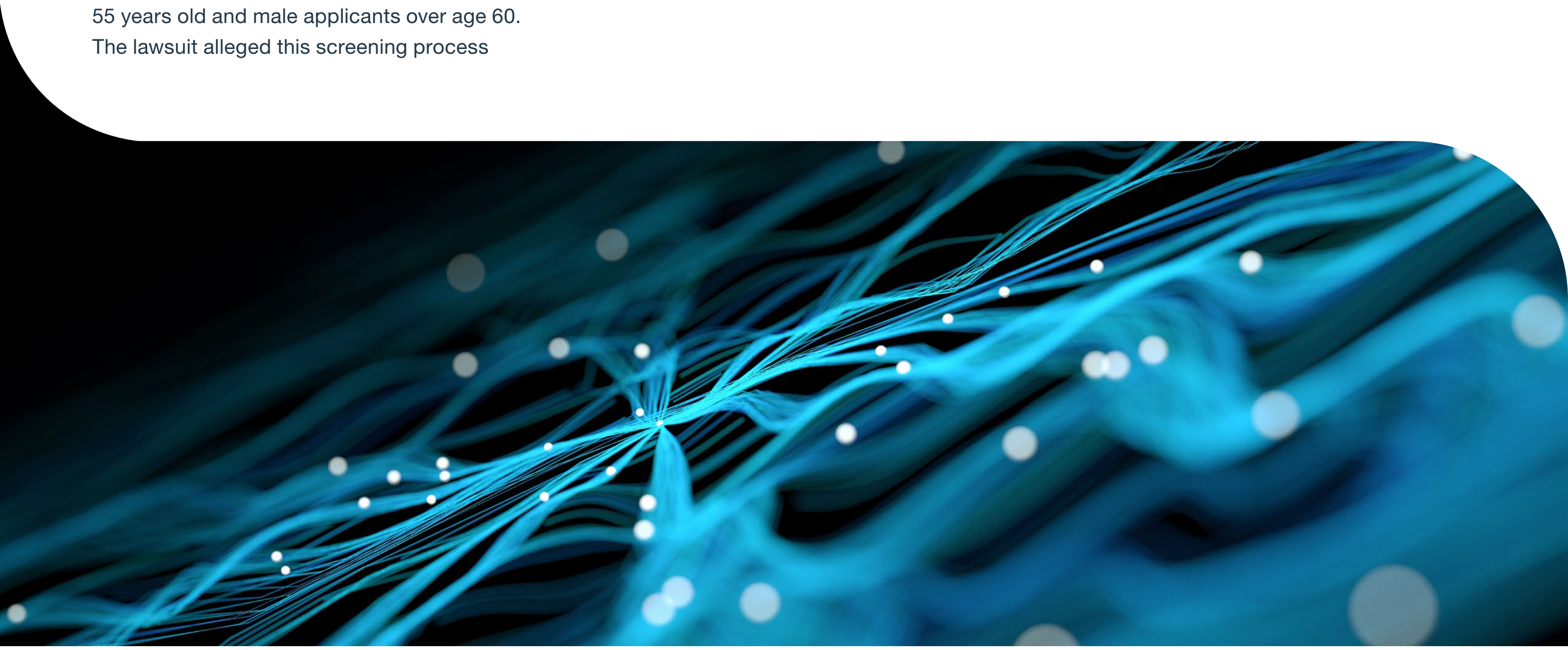
EEOC Litigation and Settlement

In May 2022, the EEOC filed an age discrimination lawsuit against a group of affiliated companies employing English-language tutors. According to the EEOC, for a brief period in the spring of 2020, those companies programmed application software to automatically reject female applicants over 55 years old and male applicants over age 60. The lawsuit alleged this screening process affected over 200 applicants who were above the programmed age thresholds. The parties reached an expansive settlement, including a consent decree subjecting the employers to various nonmonetary obligations, including providing notice of the lawsuit to high-level executives and HR employees, retaining a third-party group to conduct extensive training on all federal equal employment opportunity laws, and inviting the rejected applicants to reapply (with reporting obligations to the EEOC). It can be expected this will just be the first of many such actions by the EEOC.

Looking Ahead

The landscape in terms of the use of AI and its regulation is constantly evolving as new technologies develop and become more accessible. With many states already working on legislation to regulate AI usage, the trend can be expected to continue moving forward. The same is true in terms of litigation – both in terms of data privacy and in AI. As has already been seen, the EEOC likely will be focused on the use of AI in employment decisions, and many more lawsuits and settlements can be expected.

Employers navigating in this new arena should keep several things in mind moving forward. Consider auditing vendor AI systems that are being used for potential biased algorithms. Conduct HR and hiring manager training on the proper use of AI systems. Limit employees' access to AI tools to prevent misuse. Implement policies to limit AI use to preapproved circumstances. Provide notice to applications and employees of AI usage. Conduct privacy impact assessments to determine the risk to individuals and applicable mitigation measures. Update incident response plans to address the cybersecurity threats AI may pose to employee data. With an ever-changing world of AI, employers need to be prepared to handle the advancements and challenges that lie ahead.



International Privacy Law Update

Elizabeth (Liz) Harding
Shareholder
Denver

Christina Barnett
Associate
Chicago

Adam A. Garcia
Associate
Kansas City

Introduction

In 2023, India and Saudi Arabia each published new laws and regulations expanding on existing or setting forth new comprehensive data privacy laws. This article summarizes the notable developments in these jurisdictions, specifically focusing on the updated obligations and standards regarding cross-border transfers (i.e., when personal information is transferred from one country to another country). While organizations may already comply with some of these developments by virtue of complying with similarly instituted privacy laws, organizations should take steps to understand fully their obligations to achieve statutory compliance and minimize the risk of legal or financial liability.

India

After many years in development, the Digital Personal Data Protection Act 2023 (the "Act") was passed by the Indian Parliament in August 2023. The Act is expected to become effective in June 2024 and will supersede relevant provisions in the Information Technology Act, 2000, the Information Technology (Amendment) Act, 2008, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

This Act establishes India among the global powers with a comprehensive privacy law. However, its creation was not without challenges. India faced criticism from data fiduciaries (any organization that determines the data processing purposes and means), notably for the stringent cross-border requirements proposed in earlier drafts of the Act. The previously proposed Digital Personal Data Protection Bill 2022 (the "Bill") seemed to suggest default restrictions on cross-border data transfers, allowing only preselected countries approved by the Central Government, forming a whitelist for such countries. However, this approach significantly limited the number of approved countries, requiring the countries to match or surpass India's level of data protection and be notified by the Central Government of their approval to whitelist the respective country. The Bill also lacked specifics on how the Central Government would select and notify the white-listed countries or the terms and conditions for these transfers, including the transfers of sensitive or critical personal data that potentially affected compliance and localization requirements.[i] This uncertainty raised concerns among data fiduciaries, given India's significant role in global data processing.

The Act, however, takes a more relaxed stance on cross-border data transfers compared to the earlier Bill. As of now, the Act does not restrict the cross-border data transfers unless the Central Government notifies the specific country of the data transfer prohibition.[ii] This significant deviation from the proposed Bill allows data fiduciaries to operate without the fear of noncompliance repercussions. The Act also maintains existing sectoral laws governing industries like banking and telecommunications, preserving their restrictions on cross-border data transfers. Additionally, the Act's extraterritorial reach applies to digital personal data processing outside India if the processing is in connection with any activity referring to offering goods or services to individuals within India, aligning with global privacy laws.

It includes compliance exemptions[iii] for specific circumstances, allowing cross-border data transfers to unapproved countries and the Central Government and its agencies. Those exemptions are as follows:

- processing of personal data that is necessary for the enforcement of a legal right or claim;
- prevention, detection, investigation, or prosecution of offenses and contraventions under the Indian law;
- processing of personal data by any court or tribunal or any other body in India for judicial, quasi-judicial, regulatory, or supervisory functions;
- processing personal data of data principals outside India pursuant to a contract entered into with a foreign entity;
- processing pursuant to legally approved mergers, demergers, acquisitions, and other such arrangements between data fiduciaries; and
- processing personal data to ascertain the financial position of a defaulter to a financial institution.

Ultimately, the Act presents a broad foundation, outlining the basics of a comprehensive privacy law in India. The implementation and enforcement of the Act is expected to emerge from the Central Government in the form of rules and regulations. The Data Protection Board of India will oversee compliance with this Act and issue corrective orders and penalties for noncompliance.

[i] The Bill did not define the terms *sensitive personal data or critical personal data.*
[ii] The Digital Personal Data Protection Act 2023, Bill No. 113-C of 2023, Chapter IV §16(1).
[iii] The Digital Personal Data Protection Act 2023, Bill No. 113-C of 2023, Chapter IV §17(1).

CONTINUED ON PAGE 11 ▸

◂ CONTINUED FROM PAGE 10

Key takeaways for Organizations:

While no specific timelines for compliance have been provided, organizations should:

- Regularly review and access their data flows out of India.
- Ensure that proper data transfer agreements are in place.
- Once made available by the Central Government, regularly check the list of restricted countries to avoid non-compliance penalties.
- Non-compliance penalties could reach up to Rupees 2.5 billion (approx. $30 million).

Saudi Arabia

On September 7, 2023, the Saudi Data and Artificial Intelligence Authority issued both the Implementing Regulation of the Personal Data Protection Law (the "Implementing Regulation") and the Regulation on Personal Data Transfer outside the Kingdom (the "Transfer Regulation," and collectively with the Implementing Regulation, the "Regulations") to clarify and supplement the Kingdom of Saudi Arabia ("KSA") Personal Data Protection Law ("PDPL")[iv]. Together, the PDPL and Regulations are designed to parallel other international privacy laws and establish comprehensive data protection standards within KSA.

Cross-Border Transfers

Article 29 of the PDPL and the Transfer Regulation prescribe how data controllers[v] can legally transfer personal data[vi] outside the KSA or to a party outside the KSA. Under Article 29, data controllers may initiate such transfer if the transfer is (1) related to performing a contractual obligation where the KSA is a party, (2) to serve the interests of the KSA, (3) perform an obligation where the data subject is a party to such obligation, or (4) fulfill the purposes in the Regulations.[vii] Except in cases of extreme necessity or to prevent injuries or disease, Article 29 further requires that data transfers are only permissible when (a) the transfer will not prejudice national security or the vital interests of the KSA, (b) there is an adequate level of protection outside the KSA, and such adequacy is established by an assessment performed by a competent authority in the KSA, *and* (c) the personal data transferred is limited to the minimal amount necessary.[viii] Assuming a data controller satisfies these requirements, a data controller may legally transfer such personal data outside the KSA.

Markedly, the Transfer Regulation expands on Article 29 by describing in further detail the criteria and procedures for cross-border transfers. While the Transfer Regulation reinforces some of Article 29's requirements (e.g., by ensuring data transfers will not impact national security), the Transfer Regulation also requires data controllers to ensure the transfer does not adversely affect the level of privacy afforded to personal data.[ix] For instance, the transfer must not compromise a person's right to withdraw consent to data processing or a data controller's ability to notify data subjects in case of a data breach.[x] Further, the Transfer Regulation expands on the purposes for a transfer in Article 29 paragraph 1 by allowing data controllers to transfer personal data if (1) the transfer will enable the data controller to "carry out its activities," (2) the transfer will provide a service or benefit to the data subject, *or* (3) the transfer is for conducting scientific research.[xi] Moreover, the Transfer Regulation requires data controllers to perform risk assessments for transfers where the jurisdiction does not have adequate levels of protection or consistent transfers of sensitive data.[xii]

Additionally, the Transfer Regulation requires a competent authority (to be determined later by the Council of Ministers) to evaluate the protections of personal data outside the KSA based on enumerated criteria and recommend adequacy decisions based on such evaluations,[xiii] similar to the EU-US adequacy decision published in July 2023. These evaluations help data controllers ensure the personal data is transferred to a jurisdiction with an adequate level of protection to comply with Article 29 of the PDPL.

Finally, the Transfer Regulation provides some exceptions where a jurisdiction does not have adequate protections. If a jurisdiction does not have the adequate levels of protection, the data controller may still transfer the personal data *provided* the other jurisdiction does not prejudice the privacy of the personal data subject or the data controller's capability to implement appropriate safeguards.[xiv] In cases where a jurisdiction does not have the adequate levels of protection or a data controller cannot implement the appropriate safeguards, the KSA allows data controllers to conduct transfers so long as (1) the transfer is necessary for performing obligations where the data subject is a party, (2) the data controller is a public entity and the transfer is necessary to protect KSA's national security or for the public interest, (3) the data controller is a public entity and the transfer is necessary to investigate or detect crimes, ***or*** (4) the transfer is necessary to protect a data subject's vital interests who cannot be contacted.[xv] However, these exemptions are not applicable and a data controller must immediately stop or prevent any

[iv] Royal Decree No. M148 of 05/09/1444H, M/19 of 9/2/1443H (2023)
[v] "Controller" is defined as "[a]ny Public Entity, natural person or private legal person that specifies the purpose and manner of Processing Personal Data, whether the data is processed by that Controller or by the Processor." *Id.* at art. 1(18).
[vi] "Personal Data" is defined as "[a]ny data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature." *Id.* at art. 1(4).
[vii] *Id.* at art. 29(1).
[viii] *Id.* at art. 29(2).
[ix] The Implementing Regulations of the Personal Data Protection Law, Regulation on Personal Data transfer outside the Kingdom, chap. 1, art. 2 (2023).
[x] *Id.*
[xi] *Id.*
[xii] *Id.* at chap. 4, art. 8.
[xiii] *Id.* at chap. 2, art. 3.
[xiv] *Id.* at chap. 3, art. 5.
[xv] *Id.* at chap. 3, art. 6.

CONTINUED ON PAGE 12 ▸

◂ CONTINUED FROM PAGE 11

such transfers if (a) the transfer negatively affects KSA's national security or vital interests, (b) there is a high risk to a data subject's privacy based on the results of a risk assessment, (c) the adopted appropriate safeguards no longer apply, *or* (d) the data controller cannot enforce the appropriate safeguards.[xvi]

Compliance and Consequences

Data controllers have a one-year grace period ending on September 14, 2024, to comply with the PDPL and accompanying Regulations. Notably, the PDPL and Regulations contain other provisions in addition to cross-border transfers that address, among other things, data subject rights, information security standards, and data controller obligations regarding processers. Deliberately violating the PDPL and its Regulations with the intent to harm could result in imprisonment for two years or a fine of 3,000,000 riyals (or approximately $800,000 USD).[xvii] Other failures to comply with the PDPL and its Regulations risk fines of up to 5,000,000 riyals (or approximately $1.3 million), which may be doubled for repeat offenders.[xviii]

Key Takeaways for Organizations

Before the grace period ends in 2024, organizations should:

- Review data processing activities and privacy compliance programs;
- Update activities and programs to comply with the PDPL and its Regulations as necessary;
- Review or audit arrangements with processors/sub-processors to help ensure compliance; and
- Educate employees on obligations for the organization and themselves.

[xvi] *Id.* at chap. 3, art. 7.
[xvii] Royal Decree No. M148 of 05/09/1444H, M/19 of 9/2/1443H (2023), art. 35(1).
[xviii] *Id.* at art. 36(1).

AI for GCs: What You Need to Know for 2024

Matt A. Todd
Office Managing Partner, Licensing & Transactions Co-Chair
Houston

Reece Clark
Associate
Kansas City

Catherine (Cat) Kozlowski
Counsel
Los Angeles

Adam A. Garcia
Associate
Kansas City

Introduction

Beginning in early 2023, with the publicity and public launch of open-source and powerful, and easily applied generative artificial intelligence ("AI") tools, the interest and requests for guidance on these tools have exploded. With the spotlight has come swift change. We have been met with some surprises along the way, most notably the accelerated adoption of generative AI tools across a wide variety of applications and use cases. Never have we witnessed such a rapid adoption rate of a technology that has so many legal, business, technical, ethical, social and other considerations.

This unprecedented adoption has driven the evolving nature of both our clients' concerns and our advice. Having witnessed this evolution, we now want to (a) highlight a new and emerging issue for General Counsels ("GCs") to consider, (b) provide some interim analysis and forecast on applicable regulation and legislation, and (c) provide GCs with a framework for making "AI decisions" when presented with either a new tool or a new use case. Although there has been a veritable avalanche of AI-related content from law firms, technologists and other pundits around the world, it is our hope that our insight on these three key issues is useful for GCs in the most practical sense and provides some tools which they can deploy.

Overreliance on AI: A New Issue for GCs to Manage

While industry adoption of generative AI is still in the early days, organizations have already begun experimenting with these tools in their respective verticals.[i] This has led to some initial insights into the pitfalls of AI use (e.g., generative AI "hallucinations").[ii] In 2024, as AI continues to be operationalized at enterprise scale, GCs will need to be guarded against a new, persistent risk related to AI use: *overreliance.*

Overreliance arises when a user misunderstands the results of an AI tool or lacks understanding of how the AI tool works.[iii] Users may not, for example, be fully aware of what the AI tool can (and cannot) do, how it performs relative to the typical job functions of a human worker, or simply how

[i] Michael Chui, *The State of AI in 2023: Generative AI's Breakout Year,* MCKINSEY (Aug 1, 2023), https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year
[ii] *What are AI hallucinations,* IBM, https://www.ibm.com/topics/ai-hallucinations (last visited Dec. 20, 2023).
[iii] Samir Passi & Mihaela Vorvoreanu, *Overreliance on AI: Literature Review,* MICROSOFT (June 21, 2022), https://www.microsoft.com/en-us/research/uploads/prod/2022/06/Aether-Overreliance-on-AI-Review-Final-6.21.22.pdf.

CONTINUED ON PAGE 13 ▸

◂ CONTINUED FROM PAGE 12

the AI tool derived its results in the first place. At the same time, users may fall victim to biases of their own and the AI tools' models, and of training data that exacerbate issues of overreliance. These include automation bias (tendency to favor AI recommendations), confirmation bias (tendency to favor information derived from AI that reaffirms prior assumptions or beliefs), ordering effects (AI results that are presented early in a workflow may cause a user to anchor to those results) or overestimating the explanations provided by AI (forcing an AI to explain its results may increase the "blind trust" effect of the results).[iv]

In general, the threat of overreliance is highest where a user fails to understand how the AI tool works but recognizes that it has provided accurate results on more than one occasion. This creates a lulling effect that reduces a user's sense of urgency in validating the results upon each use. The user may find they have unwittingly accepted an incorrect recommendation, or the user may consciously or unconsciously switch their answer (in whole or in part) to match an AI recommendation even if the user had previously derived a different answer.[v]

Why is overreliance a problem? Consider the risk to people, profit and performance. In 2023, generative AI has most notably been used in marketing and sales, product and service development, and service operations.[vi] These business areas are critical to the bottom line and ensuring organization health and success. Consider the liabilities a company may face if, for example, AI incorrectly described product or service functionality (e.g., to an individual end consumer or other customer in connection with marketing materials, product labelling or contract negotiation) and overcommitted the organization, over/undersold the product or service, or gave rise to injury or damage. Or consider if an AI-derived result steers product development in a direction that is not supportable in the market or, worse, causes a latent product liability issue. These real-world examples illustrate the need to ensure accuracy and human oversight in the use of AI. AI tools may help reduce the transaction cost of information exchanges (e.g., with individual end consumers or between companies during sales, negotiation, support, maintenance and other stages), but must be monitored closely for alignment with organizational values.[vii]

What can an organization do? A popular option is to force the AI to explain how it derived a result. Yet GCs should be aware that even if an AI can provide an explanation, a user may not rigorously—or at all—check the explanation. Early studies suggest that users tend to ignore complex or lengthy explanations in favor of accepting the results blindly.[viii] As the level of complexity in the task undertaken by AI increases, so too does the complexity of the accompanying explanation. A user may believe the mere existence of the explanation (whether verified or not) will provide sufficient support. As a result, GCs need to be appropriately guarded and support policy and norm-setting exercises that rigorously evaluate the results of AI tools and AI-produced explanations.

Developing AI Regulations and What GCs Need to Know

As organizations incorporate AI into their business and operational processes, GCs must carefully navigate the litany of federal laws, initiatives and proposed regulations applicable to AI. Likewise, state laws and regulations impose additional requirements on organizations for specific data types.

There is no comprehensive U.S. federal scheme governing AI use.[ix] Instead, there is a patchwork of sector-specific consumer protection federal laws and regulations implicating AI. For instance, the Consumer Financial Protection Bureau ("CFPB") has opined that using AI could violate the Equal Credit Opportunity Act ("ECOA") where creditors rely on but do not fully understand how the AI's algorithms or "black box" elements function when they deny credit applications.[x] Additionally, the AI may discriminate or (knowingly or unknowingly) issue biased results based on race, sex or religion; creditors that exhibit automation bias violate the ECOA.[xi] The Equal Employment Opportunity Commission ("EEOC") has also released guidance indicating that employers may be liable for relying on AI that disparately impacts or discriminates against some protected classes thereby violating Title VII of the Civil Rights Act.[xii]

Meanwhile, the Securities and Exchange Commission ("SEC") and the Federal Trade Commission ("FTC") have the authority to regulate business practices related to their agency objectives,[xiii] which includes using AI in deceptive or fraudulent business practices. But their respective regulations do not readily account for intent—these agencies may rely solely on objective evidence to determine whether the AI results were deceptive regardless of how the AI was designed or used. For instance, it may be deceptive when organizations promote their use of AI to lure

[iv] *Id.* at 11.
[v] *Id.* at 3.
[vi] Chui, *supra* note 1.
[vii] *See* Reece Clark, *Frictionless Contracting In A COVID-19 Economy: Part 2,* LAW360 (July 20, 2020) https://www.law360.com/articles/1291286 citing Carl J. Dahlman, The Problem of Externality, 22 J. L. & Econ. 141, 144 (1979) ("Once the parties decide to transact, they must convey enough information to one another such that each can arrive at a reasonably agreeable bargain. This often takes time where the parties are sophisticated, and may involve external resources for information gathering.").
[viii] Katherine Miller, *AI Overreliance Is a Problem. Are Explanations a Solution?,* STANFORD UNIV. (Mar. 13, 2023) https://hai.stanford.edu/news/ai-overreliance-problem-are-explanations-solution.
[ix] See Adam A. Garcia, Note, *Socially Private: Striking a Balance Between Social Media and Data Privacy,* IOWA L. REV. 319, 329-35 (2021) (illustrating the complexities in asserting privacy rights).
[x] *Consumer Financial Protection Circular 2022-2023,* CFPB (May 26, 2022), https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms.
[xi] *Id.*
[xii] *Select Issues: Assessing Adverse Impact in Software, Algorithms, and Artificial Intelligence Used in Employment Selection Procedures Under Title VII of the Civil Rights Act of 1964,* EEOC (May 18, 2023), https://www.eeoc.gov/laws/guidance/select-issues-assessing-adverse-impact-software-algorithms-and-artificial.
[xiii] The SEC regulates any unlawful activity connected with purchasing or selling any security where a person directly or indirectly used a device to defraud or engage in any deceitful practice. *See* 17 C.F.R. § 240.10(b)-5. The FTC monitors for unfair or deceptive acts affecting commerce, and such acts are unlawful when they cause substantial injury to consumers. *See* 15 U.S. Code § 45(a)(2) (2023).

CONTINUED ON PAGE 14 ▸

◂ CONTINUED FROM PAGE 13

consumers into investment opportunities but where the investments' returns are highly misrepresented.[xiv] And misleading business practices in one instance can invite further scrutiny to an entire industry, similar to historic data collection practices.[xv]

Even if an organization complies with current applicable laws and regulations, recent federal and state initiatives may subject organizations to future regulations. The Biden Administration issued an executive order directing numerous agencies and departments to publish regulations, standards and guidelines to promote AI safety, security, data privacy, and equity and civil rights.[xvi] This executive order may drive significant changes within the federal government with respect to the use of AI tools in agency and administrative operations.[xvii] States have also created advisory councils or ordered state agencies to study and monitor how AI is used in the public and private sectors and develop policies and procedures based on those findings.[xviii] Collectively, these initiatives signal what operational and legal standards and requirements GCs should consider for their organization's use of AI.

Lastly, GCs must be cognizant of state consumer privacy laws and industry-specific regulations. For example, the consumer privacy laws in California, Colorado, Connecticut and Virginia provide consumers with the right to opt out of automated processing.[xix] Other states also regulate how AI is used in conducting job interviews.[xx] Overall, compliance may feel like a moving target, and it is. With the EU AI Act set to take effect soon, GCs must also monitor regulatory compliance abroad.[xxi] GCs may view the potential regulations yet to come, or standards from specific industries, as the sword of Damocles that will exacerbate the compliance burden. In the face of these challenges, how does a GC advise and guide in determining whether to adopt the latest new AI tool?

Evaluating AI Tools and Establishing a Method of Trust

Many aspects of AI (and particularly generative AI) are currently on unsettled ground, and early adopters may find themselves using a particular AI tool that ceases to exist a year (or five) later. Alternatively, late adopters may find themselves years behind their competitors. While the regulations and legal analyses develop with regulatory authorities and in courts, GCs can break the practical analysis into five parts:

1. What is the tool?
2. What is the use case?
3. What is the data going into it?
4. What is the output?
5. Is it accurate?

1: What is the tool?

When reviewing a novel AI tool the organization wants to use, the first question is whether it is even actually AI, using underlying machine learning. As previously noted, the FTC is already battling the misuse of the term du jour, and an effective decision tree simply does not have the same risk profile as real AI with machine learning and related models underlying it.

If the tool does in fact use machine learning, what type of model is it? Is it part of the newly exploding wave of generative AI models? Or a predictive model that has been around and in use for well over a decade?

On what data was the tool's model trained? Are there any intellectual property concerns that are currently in active litigation or likely to arise? What about bias inherited into the model from a skewed training dataset?

What are the terms and conditions? Is it a public tool, open source or an enterprise instance? Does anyone else have access to the tool's output, and if so, how might it be used? What protections is the vendor providing if, for example, the organization receives an IP infringement claim arising from use or distribution of the output content generated by the tool?[xxii]

For a risk-averse company, the analysis may end here, because the legality of how most current foundational tools and underlying models were trained is currently in active litigation,[xxiii] which can potentially impact anything generated from them, or the continued support or existence of the tool.

[xiv] *See FTC v. Automators LLC et al.,* No. 3:23-cv-01444 (S.D. Cal. Aug 08, 2023).

[xv] *See* Garcia, *supra* at 10, at 339-46.

[xvi] Exec. Order No. 14,110, 88 C.F.R. 75191 (2023). *See also Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* WHITE HOUSE (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[xvii] As a lodestar for the potential diffusion of AI technologies within federal government agencies, consider Exec. Order No. 13520 and subsequent legislative and regulatory guidance on the introduction and use of advanced information technologies to reduce fraud and improper payments. *See* Reece Clark, Note, *Kafkaesque Dangers: IPERIA, Do Not Pay, and the Government's New Fight Against Improper Payments,* 102 IOWA L. REV. 1719, 1722 (2017). *See also* Exec. Order No. 13520, 74 C.F.R. 62201 (2009).

[xviii] *Artificial Intelligence 2023 Legislation,* NAT'L CONF. OF STATE LEGISLATURES (last updated on Sept. 27, 2023), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation.

[xix] *See* CAL. CIVIL CODE §§ 1798.140(z), 1798.185(a)(16) (2023); Colo. Rev. Stat. §§ 6-1-1303(20), 6-1-13-6(1)(a)(C) (2023); 2022 CONN. PUBLIC ACT 22-15 §§ 1(22), 4(a)(5); VA. CODE ANN. §§ 59.1-575, 59.1-577(A)(5) (2023). Organizations will likely have to ensure their operations include mechanisms to receive and accommodate such requests.

[xx] In Illinois, the Artificial Intelligence Video Interview Act requires organizations to provide notice to job applicants prior to using such technology and explain how the technology will be used. 820 ILL. COMP. STAT. 42/1 (2023). Maryland also requires organizations to obtain consent prior to using facial recognition technology in job interviews. 2020 MD. LAWS., MD. CODE, LAB. & EMPL. § 3-717 (2023).

[xxi] *See The Act,* EU ARTIFICIAL INTELLIGENCE ACT, https://artificialintelligenceact.eu/the-act/ (last visited Dec. 12, 2023); Aaron M. Levine, *Is the EU AI Act Faltering,* POLSINELLI: PUBLICATIONS (Nov. 29, 2023), https://www.polsinelli.com/publications/is-the-eu-ai-act-faltering; and Aaron M. Levine, The EU AI Act, *The World's First Comprehensive AI Regulatory Scheme,* POLSINELLI: PUBLICATIONS (Dec. 12, 2023), https://www.polsinelli.com/publications/the-eu-ai-act-the-worlds-first-comprehensive-ai-regulatory-scheme.

[xxii] *Introducing the Microsoft Copilot Copyright,* MICROSOFT, https://www.microsoft.com/en-us/licensing/news/microsoft-copilot-copyright-commitment (last visited Dec. 1, 2023).

[xxiii] *See, e.g.,* Getty Images (U.S.), Inc. v. Stability AI, Inc. No. 1:23-cv-00135, at *1-4 (D. Del. Feb. 03, 2023).

CONTINUED ON PAGE 15 ▸

CONTINUED FROM PAGE 14

2: What is the use case?

AI does not solve all problems, and not all problems need AI. Evaluate the use case to which the tool will be applied and whether it is even an appropriate one for AI to address. Current/existing AI tools and their models are, at their core, prediction machines—aids relying on mathematical statistics, probabilities and correlations (not reasoning or certainty). The accuracy of that prediction can vary depending on multiple factors, as can the tolerance for, and type of, error within a use case. Detecting whether there is a bird versus a plane in an image for auto text generation has a high tolerance for error; detecting whether an abnormality in an MRI is cancerous has a far lower tolerance. Additionally, the type of inaccuracy or error—e.g., a false positive or false negative—is often critical to understanding the risks, biases and benefits. Some errors are inevitable (or even built into certain tools, machines and processes) and can be tolerated and addressed through additional processes.

Some use cases also simply do not work well with AI because individual human judgment or empathy may be necessary. An AI may share the probability of rain, but it does not know how bothered each individual may be about getting a little wet or drenched.[xxiv] Consider also whether the tool is sufficiently transparent for the use case. Again, referring to the weather example, it is unlikely that users would need to understand how the AI reached its prediction. In contrast, transparency in decision-making is critical in the employment space, and liability for determining hirings and firings may still fall on the employer's (and not the tool developer's) shoulders.[xxv]

Finally, use cases may be impacted by external factors such as legislation or industry trends. If companies use AI tools to process compliance activities, for example, overreliance presents legal risk to a company if there are errors in the results. Or consider further how overreliance on an AI tool may lead to using the tool in a setting for which it was not designed. In such a case, error rates may increase but blind trust may cause those errors to go unnoticed. Considering use cases and managing expected outcomes is critical to prevent overreliance on an AI tool that may be well suited for some tasks but not others.

3. What is the data going into it?

Data privacy and confidentiality concerns should be top of mind for GCs when reviewing a new tool. What type of information will go through the tool? Public information? Trade secrets? Will the vendor have any rights to that information as training data? Do customers have their own enterprise instance of the tool, or is that data and/or feedback flowing through a public instance? Even with a public instance, is there any risk of sensitive or trade secret data circulating through the tool showing up in a future output or influencing another customer's result?[xxvi]

4. What is the output?

The "power" of an AI's output, or risk for overreliance, can also depend on its format. Does the tool produce a report to be further analyzed by humans, an answer or decision, or perhaps a binary "yes" or "no" with little to no transparency into the probability threshold? Risk may also depend on who receives that output. Is it inward facing, for reference or additional context, or for further review? Or is it outward-facing, a result given to customers that can potentially influence their choices, even if they lack expertise in the tool's subject area?

5. Is it accurate?

Accuracy is and will be the most critical factor in analyzing any AI tool. The tool's accuracy must meet or exceed applicable thresholds based on the application (otherwise it could be more problematic than beneficial). Presumed accuracy in an AI tool is related to the concerns arising from overreliance: as the presumed level of accuracy in an AI tool increases, so does the threat of overreliance. Where an AI tool appears more accurate than not, the level of effort to check results degrades. To prevent blind trust, accuracy in AI results must not be presumed; rather, there should always be a "trust but verify" mentality that confirms accuracy and reinforces the users' understanding of the AI tool and the potential errors that may arise in use. This collectively reduces a user's tendency to blindly accept the results without further confirmation and reduces overreliance risk.

Conclusion

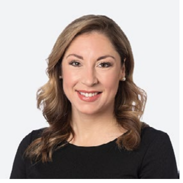
When considering the nascent regulatory field for use of generative AI in business and the potential pitfalls of AI use—most notably for 2024, overreliance and related biases—this article demonstrates that GCs will need to not only engage in norm-setting exercises to manage the use of AI in business processes but also establish a framework for AI use that reduces risk and error. That can be accomplished, in part, by using the five-factor framework in section IV above to evaluate AI tools, results and explanations objectively and critically. But internal business process management is not enough. We also anticipate GCs will implement similar checks and balances in their vendor management procedures to ensure their suppliers are conforming their services to the same rigor and safeguards when using generative AI in service delivery. A comprehensive, balanced approach will be needed as AI technology, regulations and industry-specific considerations continue to evolve. Polsinelli attorneys will continue to closely monitor the developments in AI legal frameworks and regulations and will be at the forefront in delivering timely insights to our clients.

[xxiv] Ajay Agrawal, Joshua Gans & Avi Goldfarb, *How Large Language Models Reflect Human Judgment,* HARV. BUS. REV. (June 12, 2023), https://hbr.org/2023/06/how-large-language-models-reflect-human-judgment.

[xxv] N.Y. COMP. CODES R. & REGS. tit. 20, §§ 20-870–20-874 (2023).

[xxvi] Milad Nasr et al., *Scalable Extraction of Training Data from (Production) Language Models,* ARXIV (Nov. 28, 2023), https://arxiv.org/pdf/2311.17035.pdf?ref=404media.co (prompting large language models to repeat the word "company" eventually returned the email address and phone number of a random law firm, and other similarly styled prompts returned phone numbers, emails and birthdays).

Cybersecurity Insurance: Practical Steps Your Business Can Take to Become More Insurable



Kathryn T. Allen
Technology Transactions Vice Chair
Kansas City

Kelsey L. Brandes
Associate
Kansas City

Scott M. Tobin
Associate
Chicago

With the global average cost of a data breach now $4.45 million, a 15% increase over the past three years,[i] it is not a surprise that businesses have shown an increased interest in cybersecurity insurance amid frequent news of computer hacking, network intrusions, data theft and high-profile ransomware attacks.

At the same time, there is a range of insurance policies that may cover aspects of cybersecurity incidents and crime, like stand-alone cyber policies, E&O policies, commercial general liability, D&O/management liability, commercial crime coverage, media liability, network security and privacy policies, and other blended products.

However, insurers have started writing exclusions for cyber and privacy liabilities into "non-cyber" policies and directing policyholders to buy cyber insurance specifically for those risks. **Thus, it is more important than ever for businesses to have a clear understanding of whether their current policies cover cyber incidents and, if so, to what extent. And if not, what can your organization can do as a company to make it more attractive to insurers?**

Practical Internal Steps

1. **Security Awareness Training.** We have all heard that employees are your company's greatest risk point. But with regular, documented training sessions, you can reduce this risk by educating and empowering your employees to prevent and detect common cyber threats. This also promotes a "security-aware mindset" that can have ancillary benefits. Many insurers partner with cyber-training firms and may offer them to your company at no cost. The key to success with these trainings is to be frequent and consistent.
2. **Conduct Full Data Backups.** You won't have to pay money to a cybercriminal if you have another copy of the data they are holding for ransom. The goal of regular data backups is to allow businesses to continue operating even if data is compromised. Regularly backing up all of your business data, whether it is on-premises or in the cloud, is the ultimate safety net.
3. **Automate Passwords/Use MFA.** Because most cybercriminals depend on stolen user credentials to access a private network, automated passwords and use of multifactor authentication ("MFA") could disrupt a majority of network compromise attempts. Microsoft has even gone so far as to say it would prevent 99.9% of them![ii] MFA is the process of using at least two pieces of evidence to confirm a user is who she is supposed to be (usually a password plus a one-time password or code sent to the user's phone or email). Additionally, employ a password manager to help keep track of multiple passwords and generate new passwords at random. This cuts down on employees using the same passwords for multiple platforms or writing those passwords down.
4. **Establish a Vendor Management Process.** The greatest data privacy threat companies actually faced in 2023 was their upstream and downstream vendors, with 63% of all data breaches being tied to or directly caused by vendors. Many companies rely on their procurement department to gather information and negotiate with vendors. This may be fine outside of the cyber context, but when it comes to IT, software and other vendors that have cloud-based or "connected" solutions, additional vetting and contracting processes must be employed to properly assess and mitigate the risks your vendors pose to you.

Practical External Steps

5. **Conduct Penetration Testing & System Audits.** It is important to test your company's systems, network and technical infrastructure so you find the vulnerabilities before a cybercriminal does. Often, companies that can show regular system scans and audits done by a reputable third party enjoy a break in their cyber premiums. Penetration testing is an authorized, simulated attack on your IT systems. It should be designed to mimic the techniques a cybercriminal would use to determine the efficacy of your company's security controls.
6. **Consult a Managed Service Provider.** Utilizing a third-party security professional, or managed service provider ("MSP"), to help your company better plan, monitor and secure its digital environment is an excellent way to bolster your protections. MSPs can offer 24/7 system monitoring and proactive threat detection as well as compliance management. An MSP may identify a

[i] https://www.ibm.com/reports/data-breach
[ii] https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

CONTINUED ON PAGE 17 ▸

◀ CONTINUED FROM PAGE 16

blind spot your company did not have on its radar. And as there is a crowded market for these services, they can often be the same price or less expensive than having a captive team of employees doing all of these tasks.

7. **Draft an Incident Response Plan.** No Incident Response Plan ("IRP") can guarantee the prevention of a data breach, but a well-drafted and well-rehearsed IRP can significantly minimize the impact a cyber incident has on your company. IRPs outline company procedures to follow and individual roles to engage in the event of an incident. Organizations with comprehensive IRPs had approximately $2.66 million less in damages and costs than those that did not have an IRP in place.[iii] Companies that have an IRP should review it annually. Tabletop cyber exercises bring all of the key players into the same room and have them act out what their roles and responsibilities would be if an incident were to take place. Some insurers will offer their clients a facilitator who can guide the company through this exercise. Other professional organizations should be present as well, including any MSP you have engaged and your trusted law firm partner.

With cyber insurance premiums going up and policy limits going down, as well as a consolidation of cyber insurance providers in the market, insurers want to see that their clients are engaging in industry-standard preventive measures.

Taking advantage of these practical steps will not only make companies more attractive to insurers but also improve the security posture of the company in the process, which lowers the company's need to ever claim on that policy in the first place.

[iii] https://www.ibm.com/reports/data-breach

Beyond the Blockchain: Legal Challenges and Opportunities in the Era of Digital Assets

Romaine C. Marshall
Shareholder
Salt Lake City

Jonathan E. Schmalfeld
Associate
St. Louis

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,[i] which breaks down the biggest legal developments in the blockchain, Web3 and crypto industry over the two preceding weeks.

Looking ahead, several discernible trends are surfacing that demand attention from companies actively involved in, contemplating entry into or indirectly influenced by the blockchain, Web3 and crypto sectors. The sphere of influence exerted by these emerging technologies extends far beyond the direct participants, potentially encompassing a broader range of industries and sectors than initially anticipated. This expanding impact underscores the importance for a wide array of businesses to stay informed and adapt to the evolving landscape of digital innovation.

Rise in Litigation in the Increasingly Legitimate and Valuable Industry

2023 saw an unprecedented amount of litigation in the industry, and we expect litigation will continue to rise in 2024. Thus far, the litigation has been primarily related to regulatory issues, with the three largest digital asset exchanges in the U.S. all currently subject to litigation with the Securities and Exchange Commission SEC.[ii] Additionally, a conclusion is expected in the agency's highly publicized[iii] case against Ripple Labs, Inc., with both sides securing partial victories followed by a likely appeal after the decision is finalized. The high-profile criminal prosecutions and convictions of the former heads of FTX and Binance and others have dominated 2023 news, and 2024 will likely see other or related litigation.[iv]

[i] The BitBlog Bi-Weekly can be found every other week on Polsinelli's Fintech and Digital asset blog, *available at* https://www.polsinellibitblog.com/.

[ii] *SEC v. Coinbase, Inc.*, Case No. 1:23-cv-04738 (S.D.N.Y. June 6, 2023); *SEC v. Binance Holdings, Ltd.*, Case No. 1:23-cv-01599 (D.D.C. June 5, 203); *SEC v. Payward, Inc.,* Case No. 3:23-cv-06003 (N.D. Cal. Nov. 20, 2023).

[iii] Schmalfeld, Jonathan, Will There Be a Ripple Effect? Federal Judge Rules Some Sales of XRP Were Not Securities Transactions (July 20, 2023) *available at* https://www.polsinellibitblog.com/new-blog/2023/7/20/will-there-be-a-ripple-effect-federal-judge-rules-some-sales-of-xrp-were-not-securities-transactions

[iv] *United States v. Samuel Bankman-Fried,* Case No. 22-CR-673 (S.D.N.Y. Dec. 13, 2022); *United States v. Changpeng Zhao*, Case No. CR23-179 (W.D. Wash. Nov. 21, 2023); *United States v. Braden John Karony,* Case No. CR23-433 (E.D.N.Y. Oct. 31, 2023).

CONTINUED ON PAGE 18 ▶

CONTINUED FROM PAGE 17

While regulatory litigation has been a constant in the industry, a new wave of private litigation is occurring and likely to increase, which can be expected, as industries in the billions have comparatively fewer economic incentives for litigation than do industries in the trillions, which the digital asset industry has risen into. After the digital asset market downturn in the spring of 2022, there was a wave of bankruptcy and insolvency filings and proceedings which will work their way through the courts in 2024.[v] We also expect continued growth in trademark and other intellectual property litigation,[vi] as well as private securities[vii] and ownership disputes.[viii]

As asset values go up, so do the incentives to incur litigation costs to resolve disputes over those increasingly valuable assets. With financial giants such as BlackRock and Fidelity[ix] entering the crypto space through a range of exchange-traded funds and with the growing value and use of digital assets, we expect litigation will continue to rise into 2024. 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 these lawsuits.

U.S. and International Regulation Specific to Digital Assets

Throughout the digital asset industry's growth thus far, digital assets have been forced to fit within general regulatory frameworks surrounding traditional securities and commodities. These existing regulations were designed for use of intermediary reporting mechanisms, do not address tax issues specific to barer assets like digital assets and have a variety of other shortcomings when applied to digital assets.

In short, this has led to square-peg-round-hole issues when it comes to regulating crypto. The new risks that digital assets introduce are not adequately addressed by the general regulatory framework for traditional securities and commodities. Additionally, certain historical risks which digital asset technology eliminates are also not acknowledged or reflected. As aptly stated during a congressional hearing on digital assets: "Shouldn't we take seriously the possibility that algorithms and open-source software that take a measure of human error, greed, negligence, fraud, and bias out of the system might make the system better on net even if there are some new risks that need to be examined and understood?"[x]

In the U.S., the biggest issue has been, and will continue to be in 2024, the SEC's treatment of digital assets as if they were traditional securities and thus the lack of specific rulemaking for digital assets, which are not traded or used in the ways traditional securities are traded or used. That is an issue which has been thoroughly written about.[xi] Furthermore, the SEC has recently rejected a request for rulemaking on this subject[xii] while other jurisdictions have moved forward with comprehensive digital asset regulations. It is expected that the U.S. will follow this trend to some extent in 2024.

In 2023, the European Union ("EU") passed legislation titled Markets in Crypto Assets ("MiCA") designed to govern the cryptocurrency market within its member states.[xiii] The primary objective of MiCA is to provide a harmonized set of rules across the EU for crypto assets, aimed at promoting innovation while ensuring consumer protection, market integrity and financial stability.

In the U.S., two bills regarding digital assets proceeded on a bipartisan vote through the House Financial Services Committee: the Financial Innovation and Technology ("FIT") for the 21st Century Act,[xiv] and the Clarity for Payment Stablecoins Act of 2023.[xv] In the Senate, the Lummis-Gillibrand Responsible Financial Innovation Act[xvi] and the Digital Asset Anti-Money Laundering Act[xvii] were introduced but neither passed through committee.

While none of these digital asset bills passed through Congress in 2023, that was more attributable to the general congressional backlog than to lack of motivation to get digital asset legislation passed. With fierce industry proponents (such as House Financial Services Chair Patrick McHenry) and detractors (such as Senate Banking Committee Chair Elizabeth Warren) making digital asset legislation a priority, we expect

[v] Rutenberg, Stephen, Blockchain & Cryptocurrency Laws and Regulations 2024 | False friends and creditors: The Saga of Recent Crypto Insolvencies (undated), *available at* https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/14-false-friends-and-creditors-the-saga-of-recent-crypto-insolvencies

[vi] *Yuga Labs, Inc. v. Ripps,* Case No. 2:22-cv-04355 (C.D. Cal. June 24, 2022)

[vii] *Risley v. Universal Navigation, Inc.*, Case No. 1:22-cv-2780 (S.D.N.Y. April 4, 2022).

[viii] *Anderson v. Consensus Systems, Inc.,* Index No. 655151/2023 (N.Y.S.C. Oct. 19, 2023).

[ix] *See* iShares Blockchain and Tech ETF; Depository Trust and Clearing Corporation.

[x] Statement of Brian Brooks, Digital Assets and the Future of Finance: Understanding the Challenges and Benefits of Financial Innovation in the United States (Dec. 8, 2021).

[xi] Siera, Rodrigo, Due to SEC Inaction, Registration is Not a Viable Path for Crypto Projects (March 23, 2023) *available at* https://policy.paradigm.xyz/writing/secs-path-to-registration-part-i

[xii] Gensler, Gary, Statement on the Denial of a Rulemaking Petition Submitted on behalf of Coinbase Global, Inc. (Dec. 15, 2023) *available at* https://www.sec.gov/news/statement/gensler-coinbase-petition-121523

[xiii] Regulation (EU) 2023/1114.

[xiv] Financial Innovation and Technology for the 21st Century Act, H.R. 4746, 118th Cong. (2023).

[xv] Clarity for Payment Stablecoins Act of 2023, H.R. 4766, 118th Cong. (2023).

[xvi] Digital Asset Anti-Money Laundering Act of 2023, S. 2669, 118th Cong. (2023).

[xvii] Lummis-Gillibrand Responsible Financial Innovation Act, S. 2281, 118th Cong. (2023).

CONTINUED ON PAGE 19

◂ CONTINUED FROM PAGE 18

that some industry-specific legislation will be on the agenda in 2024. Additionally, with administrative agencies moving forward with formal rulemaking, such as the IRS's proposed digital asset broker rules[xviii] and the Consumer Financial Protection Bureau's ("CFPB") proposed non-bank digital payment provider rules,[xix] we expect digital asset-focused regulation and legislation to come to the forefront in 2024.

Privacy Takes Center Role in Digital Assets

In the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, President Biden emphasizes the need to "[s]trengthen privacy-preserving research and technologies, such as cryptographic tools to preserve individuals' privacy…"[xx] At the same time, there is ongoing litigation over the Department of Treasury's sanctioning of crypto mixing service Tornado.cash[xxi] and the criminal prosecution of one of its creators, Roman Storm.[xxii]

In the late 1990s, with the rise of email, there was also an attempt to regulate the publication and exportation of privacy-preserving cryptographic technologies so they wouldn't be used by terrorists and other bad actors to avoid government surveillance. The result of those laws and associated challenges was *Bernstein vs. DOJ,*[xxiii] in which the Ninth Circuit recognized the proposition of "code-is-speech" and that any attempt to regulate the mere publication of computer code must pass the heightened scrutiny test required for government regulation of otherwise constitutionally protected speech.

While the ruling in *Bernstein* was for First Amendment protections, there is often overlooked *dicta* in the case which states: "the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously, the right against compelled speech, and the right to informational privacy."[xxiv]

The Bank Secrecy Act, the Patriot Act and a large number of the financial surveillance regulations currently in place are predicated on the assumption that people always need intermediaries to transact and thus surveillance can be done at the intermediary level. This is extended under the "third-party doctrine," which is the legal principle that a party lacks a reasonable expectation of privacy under the Fourth Amendment over information "revealed to a third party and conveyed [by that third party] to the Government authorities."[xxv]

While transfers of (most) cryptocurrencies occur on public and immutable blockchains, the records of which are available to all, these transactions are done through largely anonymous digital wallets free of any centralized intermediaries which could be regulated. Additionally, the creation of these wallets does not depend on any intermediary, and creation of a compatible digital wallet on most blockchain networks can be done with publicly available computer code and a random number generator.

We expect to see in 2024 an intense discussion and debate about whether the government can and should seek to impose financial surveillance at a more direct level and at an individual level, as opposed to the financial intermediary level consistent with historical practices. The rights of individuals to transact in digital assets through the use of privacy-preserving technologies such as zero-knowledge proofs, cryptocurrency mixing protocols, virtual private networks and anonymous digital wallets will be at the forefront of regulations and litigation in 2024.

Conclusion

The landscape of digital asset litigation and regulation is evolving rapidly, reflecting the dynamic nature of this burgeoning industry. As digital assets gain legitimacy and value, they attract more regulatory scrutiny and private litigation. The industry's fit within existing regulatory frameworks remains a square-peg-round-hole dilemma, particularly in the U.S. Internationally, however, strides are being made with comprehensive regulations like the EU's MiCA.

In the U.S., despite stalled legislation in 2023, there is a growing momentum for industry-specific laws and regulations in 2024, with key figures in Congress and various administrative agencies taking active roles. Privacy issues, particularly regarding transactions in digital assets, are set to take center stage, challenging traditional regulatory assumptions and possibly reshaping the legal landscape. This evolving regulatory and litigation environment underscores the need for specialized legal expertise in navigating the unique challenges and opportunities presented by digital assets.

[xviii] Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions, Proposed Rule by IRS (Aug. 29, 2023), *available at* https://www.federalregister.gov/documents/2023/08/29/2023-17565/gross-proceeds-and-basis-reporting-by-brokers-and-determination-of-amount-realized-and-basis-for

[xix] Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, Proposed Rule by CFPD, (Nov. 7, 2023) *available at* https://www.consumerfinance.gov/rules-policy/rules-under-development/defining-larger-participants-of-a-market-for-general-use-digital-consumer-payment-applications/

[xx] Exec. Order No. 14110, 88 FR 75191 (Oct. 30, 2023).

[xxi] *Van Loon v. Dept. of Treasury,* Case No. 23-50669 (5th Cir. Nov. 13, 2023).

[xxii] *United States v. Roman Storm,* 23-CRIM-430 (S.D.N.Y. Aug. 23, 2023).

[xxiii] *Bernstein v. United States Department of Justice,* 176 F.3d 1132 (9th Cir. 1999)

[xxiv] *Id.* at 1146.

[xxv] *United States v. Miller,* 425 U.S. 435, 443 (1976).

The SEC Raises the Stakes: New Cybersecurity Rules for Publicly Traded Companies Hit the Books in 2023

Pavel (Pasha) A. Sternberg
Principal
Los Angeles

Caitlin A. Smith
Associate
Washington, D.C.

Overview

In 2023, the U.S. Securities and Exchange Commission ("SEC") issued its now-fully implemented Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule. The Rule reflects the reality that cybersecurity is now a major operational issue for companies and seeks to standardize the disclosures of cyber incidents and overall cyber risk management for publicly traded companies. It also marks a significant expansion of what information about their cybersecurity posture those companies must make public through their annual disclosures as well as in one-off 8-K disclosures in the event of a data security incident.

The Rule creates a few major requirements:

1. **Disclosure of a Registrant's Risk Management, Strategy and Governance Regarding Cybersecurity Risks:** Companies must proactively include information about their processes for assessing, identifying and managing material risks from cybersecurity threats in their annual disclosures. Additionally, companies need to disclose if risks from cybersecurity threats, including those stemming from previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company. These disclosures must be made in a way that reasonable investors can understand, with the idea being that investors are increasingly factoring in a company's cybersecurity posture when deciding whether to invest in that company.
2. **Disclosure Regarding the Board of Directors' Cybersecurity Expertise:** Companies must also describe management's role in assessing and managing material risks from cybersecurity threats, as well as the Board of Directors' oversight of these issues. This latter disclosure should identify the management positions responsible for assessing and managing the risks; the relevant expertise of the individuals in those positions; the processes by which management is informed about and monitors the prevention, detection, mitigation and remediation of cybersecurity incidents; and the threshold for management to escalate cyber risks to the Board or Board Committee. The purpose behind this separate disclosure is to give investors insight into not just a company's technical cybersecurity posture but also how much the senior levels of the company are factoring cybersecurity in their management decisions.
3. **Timely Disclosure of Cybersecurity Incidents:** Companies must disclose cybersecurity incidents (usually in a Form 8-K filing) within four business days of determining they have experienced a "material" incident. The materiality of an incident must be determined "without unreasonable delay" and by considering factors such as the incident's impact on the company's reputation; customer or vendor relationships or competitiveness; and the possibility of litigation or regulatory investigations. In essence, materiality will be determined in a similar way as other 8-K filings – whether the incident could influence the investment decision of a reasonable shareholder. Once the materiality threshold is met, the disclosure must describe the nature, scope and timing of the incident, as well as the "material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations." The disclosure must also be amended as additional material information is discovered after the initial filing.
   - **Note:** the Rule has a built-in appeal process to delay this disclosure if the U.S. Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety. This process involves the Federal Bureau of Investigation ("FBI"), the Department of Justice ("DOJ") and the SEC, all of which have issued guidance on their portion of the process. Although time will tell, based on these guidance documents, it is likely that an exception is rarely going to be given.
   - **Another Note:** the SEC is not exempting companies from providing disclosures regarding cybersecurity incidents on third-party systems they use. Depending on the circumstances of an incident that occurs on a third-party system, disclosure may be required by both the service provider and the customer of those services, by one or the other, or by neither.
   - **A Final Note:** threat actors are clearly aware of the SEC's expectation that incidents are reported quickly, as there have already been a few instances where the threat actors who attacked a company then subsequently reported the attack to the SEC after their victims failed to do so. This tactic is clearly aimed at putting additional pressure on the company as it navigates its response to the threat actor's attack.

How to Comply

In response to the new Rule, companies should review their overall cybersecurity posture, their cybersecurity management programs, and their incident response procedures. Specifically, companies subject to the Rule should focus on a few areas of work:

CONTINUED ON PAGE 21 ▸

◂ CONTINUED FROM PAGE 20

Enterprise-Wide Cybersecurity Strategy

Gone are the days when IT could be siloed off and asked to "handle the technical stuff." Companies now need to have an in-depth cross-department strategy for handling cybersecurity. That strategy also needs to be regularly tested, evaluated and revised. This requires an organization with a cybersecurity governance structure that is empowered and held accountable at the highest levels of the organization and which trickles down throughout the company.

Board Training

With the Rule's requirement that organizations demonstrate their Board's proficiency and oversight of cybersecurity risks, the Board should get adequate reports and presentations on the general cyber threat landscape and what the organization is doing in response to that landscape.

Cyber Incident Response Planning and Testing

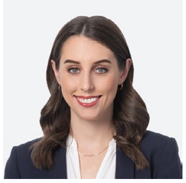
By planning ahead and properly preparing for a cybersecurity incident, an organization can respond to an actual incident in a more efficient and strategic way. In doing so, it may be able to keep an incident from becoming material and therefore reportable. Companies need to assess and implement an enterprise-wide Incident Response Plan ("IRP"). A good IRP addresses how the entire organization will respond to an incident. Limiting an IRP to the IT and security team's role results in the organization not taking into account all of the business, legal and messaging decisions that need to be made during a cyber incident. Once an IRP is developed, it should be tested through regular tabletop exercises.

Additionally, executive leadership should think through the materiality standard for cyber incidents. While materiality is not a new concept for 8-K purposes, the short timelines imposed by the Rule mean that quickly making this determination in the midst of a data incident will be challenging. Companies need to think ahead to consider the current threat landscape and how particularly disruptive incidents, like ransomware, may impact the organization operationally, financially and reputationally.

Business Continuity Planning and Testing

Ransomware is one of the most common types of cyberattacks and is the most disruptive to an organization. It is therefore the one most likely to create a material cyber incident. As a result, organizations need to implement and regularly test a business continuity plan and backup systems. This extends to plans for events involving third-party vendors.

It's Not Your Fault, but It May Be Your Problem: Increasing Regulatory Scrutiny on Vendor Cybersecurity Risks



Kayleigh S. Shuler
Associate
Kansas City

For organizations that watched (or worse, lived through) the fallout from recent large-scale vendor incidents, the prospect of learning that a trusted vendor has experienced a data incident is almost as distressing as the idea of the organization experiencing an incident itself.

That's because a vendor incident – meaning an incident that occurs at or is otherwise caused by a third-party service provider – can be nearly as time-consuming, costly and reputationally damaging as an internal incident.

Challenges of Vendor Incidents

Vendor incidents can come with all the usual challenges of any security event – operational disruptions, public relations pressures and concerns about data compromise – but often come with the added element of being "in the dark" until a vendor decides to share details about what happened and what they're doing about it. Additionally, depending on the vendor's level of cooperation, the ultimate responsibility to notify individuals may land on the company, even though it is not at fault. All the while, an individual who learned that their data may have been compromised will likely point the finger back at whomever they entrusted their data to, regardless of whether that company is truly where the breach occurred.

Increasing Regulatory Attention

Regulatory bodies, particularly those in the financial industry, are increasingly taking note of this type of incident and raising the level of attention they pay to vendor management. Questions that often come after a company notifies regulators of a vendor incident include: What level of diligence did your organization conduct before trusting a vendor with data? If the vendor made security-related promises – such as to delete data after contract termination – did your organization confirm those promises were kept? Why was a vendor holding so much data for so long?

In 2023, we saw regulatory efforts to gain more insight into these relationships and the risks they pose in the National Credit Union Administration's ("NCUA") approval of a final rule that requires a federally insured credit union to report "reportable cyber incidents" to the NCUA as soon as possible, and in no event later than 72 hours after the credit union reasonably believes that it has experienced a reportable cyber incident.[i] Under the rule, the NCUA suggests that if a *third party* reports experiencing a breach of a credit union's sensitive member information, that

[i] 12 CFR § 748.1(c).

CONTINUED ON PAGE 22 ▸

◂ CONTINUED FROM PAGE 21

credit union likely needs to report to incident to NCUA.[ii] Credit unions have apparently heeded that advice. According to NCUA Chairman Todd M. Harper, "[i]n the first 30 days after the rule became effective, the NCUA received 146 incident reports, more than it had received in total in the previous year. More than 60 percent of these incident reports involve third-party service providers and credit union service organizations."[iii]

Regulators overseeing banks have so far approached the issue from a slightly different and less direct direction but with a similar result. In guidance issued June 6, 2023, the Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve System and the Office of the Comptroller of the Currency (the "Banking Agencies") provided detailed guidance to banking organizations on vendor management throughout the life cycle of a vendor relationship. This guidance included oversight and accountability procedures for the life of the relationship.[iv] This guidance added to an existing rule issued from the Banking Agencies which requires bank *service providers* to notify bank customers as soon as possible upon experiencing certain types of incidents.

Looking Ahead

Looking ahead to 2024, we can expect continued vendor incident scrutiny on both vendors and the organizations they serve. For its part, the NCUA is currently seeking congressional authority to directly examine third-party vendors, which it cannot do under existing law.

In testimony before Congress, the NCUA has stated that its inability to directly regulate credit union providers "creates a regulatory blind spot"[v] and that without this power, "NCUA is unable to effectively protect credit unions and their members."[vi] If Congress agrees, the NCUA may be given authority to demand information from vendors or impose corrective action plans on them, which vendors can largely ignore under current law.

Given the frequency with which vendor incidents are occurring and the increased regulatory interest in them, organizations should think through what they can do to position themselves for a strong response. For instance, consider: If a regulator inquired about how we vetted a vendor, are we comfortable with our answer? Is our vendor management program robust?

For those on the vendor side of the coin, the challenges are similar, but the key questions are different. Here, consider: if customers impose additional security vetting, are we prepared to provide the accurate and digestible information they'll need to feel comfortable partnering with us?

In all cases, as we head further into 2024, increasing regulatory attention to vendor security should be top of mind.

[ii] *See,* Appendix A: Examples of Substantial Incidents that Likely Would Qualify as Reportable Cyber Incidents, available at https://ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/cyber-incident-notification-requirements/appendix-a

[iii] *See,* testimony of NCUA Chairman Todd M. Harper Before the Senate Banking, Housing, and Urban Affairs Committee, available at https://ncua.gov/newsroom/testimony/2023/ncua-chairman-todd-m-harpers-written-testimony-senate-banking-housing-and-urban-affairs-committee#:~:text=In%20the%20first%2030%20days,union%20service%20organizations%20(CUSOs).

[iv] *See,* Interagency Guidance on Third-Party Relationships: Risk Management; https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf

[v] *See,* testimony of NCUA Director of Office of Financial Technology and Access Charles A. Vice before the Subcommittee on Digital Assets, Financial Technology and Inclusion

[vi] Harper testimony, *supra* note 3.

Looking Ahead to the FTC's Implementation of the Data Breach Notification Rule for Nonbanking Financial Institutions

Alexander D. Boyd
Shareholder
Kansas City

Colin H. Black
Associate
Chicago

Beginning on May 13, 2024, nonbanking "financial institutions" must notify the Federal Trade Commission ("FTC") within 30 days of discovering a data breach involving the nonpublic personal information of at least 500 consumers. These covered organizations can include a wide variety of companies that engage in financial activities but that are not directly regulated by federal banking regulators, including automobile dealerships, higher educational institutions participating in federal student financial aid programs, mortgage lenders or brokers, tax preparation firms, travel agencies, and others. These organizations are already required to implement certain information security protections pursuant to the FTC's Safeguards Rule.[i] The FTC's new data breach notification requirement will provide the FTC with a critical tool to ensure that organizations are properly safeguarding consumer data.

Background

All fifty states have enacted some form of a data breach notification law. Certain industries are also subject to data breach notification obligations at the federal level. The Gramm-Leach-Bliley Act ("GLBA") imposes certain privacy and data security obligations on covered "financial institutions."[ii] Under the GLBA, financial

[i] 16 C.F.R. Part 314.

[ii] 15 U.S.C. §§ 6801-6809.

CONTINUED ON PAGE 23 ▸

CONTINUED FROM PAGE 22

institutions are broadly defined to include any institutions engaging in activities that are financial in nature or incidental to such financial activity.[iii] For banking (typically depository) financial institutions, the GLBA provides enforcement authority to the federal banking regulators (the Federal Deposit Insurance Corporation, Federal Reserve, Office of the Comptroller of the Currency, and National Credit Union Administration). For all other types of financial institutions, the GLBA provides enforcement authority to the FTC.[iv]

Under the FTC's existing Safeguards Rule, covered financial institutions must develop, implement and maintain an information security program that includes nine specific elements.[v] On October 27, 2023, the FTC adopted an amendment to the FTC's Safeguards Rule that will increase the number of organizations subject to federal data breach reporting requirements, including many organizations that may not realize they are considered a "financial institution" under the GLBA's broad definition.

Requirements Under the Amended Safeguards Rule

The amended Safeguards Rule requires financial institutions to report any instance of the unauthorized acquisition of unencrypted customer information of at least 500 consumers to the FTC as soon as possible but in no event later than thirty days following discovery of the incident. The rule broadly defines customer information to include any nonpublic personal information about a customer of a financial institution, whether in paper, electronic or other form.[vi] This includes any information provided by the customer in order to obtain a financial product, information about a customer resulting from any transaction involving a financial product or service, and any other information obtained about the customer in connection with providing the financial service.

The notice to the FTC must include (1) the name and contact information of the reporting financial institution, (2) a description of the types of information that were involved in the notification event, (3) the date or date range of the notification event (if it is possible to determine), (4) the number of consumers affected, (5) a general description of the event, and (6) if applicable, whether any law enforcement official has provided the institution with a written determination that notifying the public of a breach would impede a criminal investigation.

Anticipating FTC Investigations and Public Disclosure Under the New Rule

Once an organization notifies the FTC of a data breach under the new rule, it will then face risks associated with the public disclosure of the notice and a potential FTC investigation. The FTC intends to publicly post the data breach notices it receives.[vii] These postings will increase the risk of litigation and media attention arising out of the data incident.

The FTC is also likely to initiate investigations into many of the reported breaches.[viii] Consistent with how the FTC has investigated prior data security incidents and consistent with how other federal regulators investigate reported incidents, reporting organizations should expect the FTC to conduct a three-pronged inquiry following a data breach report. First, the FTC will likely request information about how the organization responded to the incident, including how it conducted its investigation, how it ensured that its systems were secure, and whether and how it notified potentially affected individuals. Second, the FTC is likely to seek information about the organization's underlying information security program and compliance with the FTC's Safeguards Rule. Finally, the FTC may seek information about the organization's overall data privacy compliance program under the FTC's jurisdiction to investigate and prohibit unfair or deceptive acts or practices in commerce.[ix] The FTC's inquiry into these areas can be quite detailed.

Preparing for the New Rule

As a threshold matter, all organizations should determine whether they are subject to the FTC's Safeguards Rule well in advance of any data security incident. The new data breach notification requirement is only one part of the more comprehensive set of data security requirements under the Safeguards Rule. Covered organizations must implement an information security program that contains nine specific elements. This new reporting rule provides the FTC with a new method to identify and investigate financial institutions that may not be compliant with the Safeguards Rule.

Covered organizations should ensure that their data security incident response plans address the new rule by incorporating the definitions and reporting time frames under the FTC rule and other applicable law. As with any external notice regarding a data security incident, notices to the FTC should be timely, factual and accurate. The organization should identify the person or team who will be responsible for leading the organization's incident response and ensuring that regulators are notified in accordance with applicable law.

The organization should distribute the updated incident response plan to all individuals who may be required to execute on the plan in both physical and digital formats. Once the plan is adopted, organizations should ensure that the plan is routinely tested to identify potential gaps and to increase the effectiveness of the response plan under an actual crisis.

[iii] 15 U.S.C. § 6801(3).
[iv] 15 U.S.C. § 6805.
[v] 16 C.F.R. § 14.4
[vi] 16 C.F.R. § 314.2.
[vii] 88 Fed. Reg. 77,506 (Nov. 13, 2023).
[viii] 88 Fed. Reg. 77,501 (Nov. 13, 2023).
[ix] 15 U.S.C. 45.

Stay Connected

Polsinelli frequently writes about topics related to these materials. Click here to subscribe to receive news and webinar updates.

About Our Technology Transactions & Data Privacy Practice

Polsinelli's Technology Transactions and Data Privacy team is comprised of over 50 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.

Editorial Board

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

polsinelli.com | Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.