2024 YEAR IN REVIEW

Year in Focus: Key Cybersecurity and Privacy Developments in 2024

Paul, Weiss, Rifkind, Wharton & Garrison LLP

Paul | Weiss

January 23, 2025

Year in Focus: Key Cybersecurity and Privacy Developments in 2024

As we entered 2024, the cybersecurity and data privacy landscape was evolving at a rapid pace as companies worked to keep pace with pervasive cyber threats and evolving regulatory measures. Threat actors continued to find success in 2024. Headline-grabbing incidents impacted industries ranging from healthcare to telecommunications, ransomware remained a persistent threat – including a record $75 million ransom payment – and attacks against cloud services had downstream impacts for hundreds more victims companies.

Concurrently, regulators pursued aggressive theories of liability under the securities and other laws, securing hundreds of millions of dollars in fines, and proposed a slew of new regulations addressing incident disclosure, security requirements and international data transfers. These efforts come as both companies and regulators also focus on also how to address legal complexities introduced by the integration of advanced technologies such as artificial intelligence into everyday business operations.

In this dynamic environment, the Paul, Weiss Cyber & Data Protection team has identified **ten key developments of 2024** that have shaped the legal and data security landscape – developments that pose new challenges and are driving business leaders to allocate more resources to meet the evolving threat and legal requirements.

Looking ahead, the cyber threat will endure even amidst uncertainty as to the Trump administration's approach to cybersecurity policy. We expect a continued focus on critical infrastructure security and aggressive pursuit of foreign cyber actors, especially where there is intersection trade policy or other administration priorities. Even in a deregulatory environment at the federal level, we expect that 2025 will see continued activity from threat actors and state and international regulators.

1. SEC cyber incident disclosure rule brings additional SEC guidance

New Securities and Exchange Commission ("SEC") rules that require public companies to disclose material cybersecurity incidents under new Item 1.05 of Form 8-K went into effect for most companies on December 18, 2023.

In response, many companies erred on the side of providing early disclosure. While Item 1.05 is only triggered once a company determines an incident to be material, the first half of 2024 saw companies repeatedly disclosing under Item 1.05 but stating that either they had not determined the incident was material or, in some cases, had determined the incident was not material. In the months after the rule took effect, more than a dozen companies disclosed incidents under Item 1.05 that the companies had not yet determined were material – and therefore did not require disclosure under Item 1.05. Of the first eleven companies to file Forms 8-K to report a cybersecurity incident under Item 1.05, only two identified a material impact.

In response, the SEC's then-Director of the Division of Corporation Finance Erik Gerding published a statement urging public companies to report only material cyber incidents under the SEC's new cybersecurity rules. Gerding encouraged companies to disclose incidents not deemed material under a different item of Form 8-K, such as Item 8.01 (Other Events). Gerding did not suggest that incidents not deemed material should not be disclosed, rather he "recognize[d] the value of such voluntary

disclosures to investors, the marketplace, and ultimately to companies, and [his] statement is not intended to disincentivize companies from making those disclosures." If all cybersecurity incidents are disclosed under Item 1.05, then there is a risk that investors will misperceive immaterial cybersecurity incidents as material, and vice versa, Gerding explained.

In light of Gerding's comments, public companies must carefully consider the item of Form 8-K under which they disclose cybersecurity incidents. Gerding acknowledges that early, voluntary disclosures have value to investors and the marketplace, but his statement is a reminder that such early disclosures are not the end of the analysis. Even if a company made an early disclosure, once it determines that an incident is material the company must disclose the material impact of the incident in a subsequent filing that satisfies all of the requirements of Item 1.05.

Gerding was not the only SEC official to offer guidance on the new reporting requirements. On June 24, 2024, the staff of the Division of Corporation Finance released five new Compliance & Disclosure Interpretations relating to the disclosure of material cybersecurity incidents under Item 1.05 of Form 8-K.

- **The completion of a ransomware attack does not moot the materiality determination**: If, prior to any materiality determination by a registrant, the registrant pays the ransom and the threat actor ends their disruption of operations and returns any exfiltrated data, the registrant must still make a determination regarding the incident's materiality.

- **Material cybersecurity events, even if completed, must still be disclosed**: Even if a cybersecurity incident is resolved prior to the required filing of the Form 8-K, a cybersecurity incident determined to have a material impact or that is reasonably likely to result in a material impact on the registrant must still be disclosed.

- **Insurance policies and reimbursement**: Reimbursement for a ransomware payment under a registrant's insurance policy does not mean that a cybersecurity incident is immaterial.

- **Size of Ransomware Payment**: The size of the ransomware payment is only one fact relevant to a registrant's materiality determination and, by itself, is not determinative.

- **Related Cybersecurity Events**: A series of cybersecurity incidents, if related, may be material in the aggregate, even if individually any single incident was not material.

In 2025, we expect that companies will continue to grapple with how to assess materiality and disclose cybersecurity incidents in only the second year of required reporting under the SEC cyber incident disclosure rule.

2. SEC dealt blow in litigation against SolarWinds for allegedly deficient cybersecurity disclosures and controls

In 2024, the SEC suffered a significant setback in *SolarWinds*, one of its highest profile actions related to cybersecurity. In 2023, the SEC had filed an action against SolarWinds and its Chief Information Security Officer (CISO) related to a cybersecurity incident known as SUNBURST. The attack was conducted over nearly two years by Russian-backed hackers and is considered one of the worst cyber-incidents in U.S. history, exacerbated by the fact that several U.S. government agencies relied on SolarWinds software.

When filed, the SEC case against *SolarWinds* case marked a number of firsts for the SEC: the first time it had brought intentional fraud charges in a cybersecurity disclosure case, the first time it had brought an accounting control claim based on an issuer's alleged cybersecurity failings, and the first time it had brought a cybersecurity enforcement claim against an individual. The SEC alleged that SolarWinds and its CISO defrauded the company's investors and customers through misstatements, omissions and schemes that concealed both SolarWinds's purportedly poor cybersecurity practices and its increasing cybersecurity risks, including a security statement published on the company's website, in a cybersecurity risk disclosure made in SolarWinds's SEC filings, and in press releases, podcasts and blog posts.

On July 18, 2024, Judge Paul A. Engelmayer of the U.S. District Court for the Southern District of New York granted in large part a motion to dismiss the SEC suit. The motion to dismiss was supported by several groups that submitted amicus briefs, including a brief submitted by Paul, Weiss on behalf of former government officials. The only set of claims sustained by the court were the claims for securities fraud based on the security statement on the company's website, which claims the court held were viably pled as materially false and misleading.

The July 18, 2024 ruling included several key takeaways for companies:

- **Specific false or misleading statements on a company's public website about the state of a company's cybersecurity can be the basis for securities fraud liability**: The fact that these claims based on a public security statement were the only claims to survive the motion to dismiss serves as an important reminder that all public statements about a company's cybersecurity practices, not only those in SEC filings, can have legal consequences and should therefore be carefully reviewed for accuracy.

- **Cybersecurity risk disclosures and disclosure controls can provide important defenses to securities fraud claims**: In the court's view, "[p]erspective and context are critical" when evaluating whether SolarWinds's Form 8-K was sufficiently pled as materially misleading; considering the "short turn-around" in which SolarWinds was able to file its Form 8-K disclosing the SUNBURST attack, it contained "appropriate gravity and detail."

- **"Internal accounting controls" do not extend to cybersecurity controls**: "Cybersecurity controls," stated the court, "are undeniably vitally important, and their failures can have systemically damaging consequences. But these controls cannot fairly be said to be in place to 'prevent and detect errors and irregularities that arise in the accounting systems of the company.'" If the decision stands, it could limit the SEC's ability to pursue Exchange Act claims related to internal controls that do not relate specifically to the company's financial statements. And it will certainly make it more difficult for the SEC to settle internal accounting controls claims based on allegedly efficient cybersecurity controls, such as when just a month prior to the *SolarWinds* decision R.R. Donnelley & Sons Co. agreed to pay $2.1 million to settle charges that the company failed to maintain "cybersecurity-related internal accounting controls" and to design effective disclosure controls to report relevant cybersecurity information to management.

3. Despite *SolarWinds* setback, SEC settles with four companies regarding their cybersecurity disclosures

The continued *SolarWinds* litigation was but one example of the SEC's efforts in 2024 to police companies' cybersecurity disclosures. On October 22, 2024, the SEC announced charges against four current and former public companies related to the companies' respective disclosures following cybersecurity incidents involving the supply-chain compromise of SolarWinds software. In its announcement, the SEC said that each company "negligently minimized its cybersecurity incident in public disclosures, . . . leaving investors in the dark about the true scope of the incidents." The charges, for example, alleged that statements in some companies' annual filings were materially misleading because the statements described known cybersecurity events as hypothetical and described a known intrusion and risks in generic terms. The SEC also alleged disclosure controls and procedures violations. Some companies faced charges that their disclosures attempted to minimize the scope of the intrusion and the nature of the information exposed. To settle the SEC's charges, each company agreed to cease and desist from future violations and to pay civil penalties ranging from $990,000 to $4,000,000.

The coordinated announcement of these four actions highlights the SEC's continued efforts to encourage robust disclosures to investors regarding cybersecurity risks and incidents. Information the SEC may expect to see in disclosures includes:

- **Quantification of an incident's impact**: The SEC explained that it expected the companies to quantify the information or customers impacted and to clearly identify the categories of affected or exfiltrated data. One company's Form 8-Ks, "negligently created a materially misleading picture of the Compromise, providing quantification regarding certain aspects of the Compromise but not disclosing additional material information on the scope and impact of the incident."

- **Identity of the threat actor, timeline of the intrusion, and other details**: The SEC faulted one company for not disclosing a variety of specific details that the SEC determined—without significant analysis—to be material, including "the likely attribution of the activity to a nation state-state actor, the long-term unmonitored presence of the threat actor in [] systems, the access to at least 145 shared files some of which contained confidential and/or proprietary information, and the fact that the mailbox the threat actor accessed belonged to [] cybersecurity personnel."

- **Confirmation of an incident's occurrence**: The SEC faulted the companies for failing to clearly state that an incident had occurred, instead describing the possibility of incidents in generalized or hypothetical terms. The SEC also took note of where the companies repeated language used in prior filings after they had identified potentially material incidents that, in the SEC's view, changed the companies' cybersecurity risks.

- **Gaps in available forensic evidence:** While caveats and phrases like "based on available evidence" are often necessary to account for the uncertainty inherent in cybersecurity investigations, the SEC suggested in one order that some gaps or limitations in available forensic data are material and must be disclosed. For example, one company only had relevant logs for a four-month period and did not have logs of activity that could have occurred before that timeframe, "which prevented it from identifying the full scope of the compromise." The SEC believed that "there is a substantial likelihood that a reasonable shareholder would consider" the company's "inability to fully assess the scope of activity . . . important when evaluating . . . statements about intrusions and their impact on the company."

- **Consideration of industry-specific risks:** Importantly, all four of the companies are technology companies. Each of the SEC's orders emphasized that for companies providing IT or cybersecurity services, risks to protections for networks and data could be material because those abilities are essential to such companies' reputations and ability to attract customers. But the SEC might evaluate the reputational risk of a cybersecurity incident – and therefore the overall material impact of an incident or the materiality of specific facts about an incident – differently for victim companies in different industries.

4. DOJ proposes rulemaking to restrict the transfer of certain sensitive U.S.-person data

On October 21, 2024, the National Security Division of the U.S. Department of Justice ("DOJ") issued a notice of proposed rulemaking ("NPRM") to restrict or prohibit the sharing of certain U.S.-person data with "countries of concern": China, Cuba, Iran, North Korea, Russia and Venezuela. Only three months later, on December 27, 2024, DOJ issued the final rule.

The rule regulates whether and how U.S. persons can engage in "covered data transactions" with "covered persons." "Covered data transactions" include transactions involving a data brokerage, a vendor agreement, an employment agreement or an investment agreement. The rule applies to both transactions involving "sensitive personal data" and U.S.-government-related data. "Covered persons" include foreign entities, employees, contractors or individuals with specified relationships to countries of concern, as well as persons or entities designed by the Attorney General. The rule restricts certain covered transactions by requiring U.S. persons to comply with security requirements promulgated by the Cybersecurity and Infrastructure Security Agency ("CISA"), and prohibits other covered transactions altogether.

The final rule creates a significant new regulatory regime for data security that will affect the operations of many companies in the data-driven economy. It will impact U.S. companies' ability to pursue certain data sharing partnerships and arrangements with China and other countries of concern. Companies will also need to establish internal compliance programs to ensure their transactions – and the transactions of their counterparties – conform with the rule and CISA security requirements. Assistant Attorney General for National Security Matthew Olsen provided four points of advice to companies preparing for the rulemaking: (1) know your data, (2) know where that data is going, (3) know who has access to the data, and (4) know your data sales.

5. CISA proposes sweeping cyber incident reporting rule

On March 27, 2024, CISA released a long-anticipated notice of proposed rulemaking ("NPRM") setting out its initial approach to new reporting requirements under the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"). CIRCIA created a

mandatory federal cyber-incident reporting regime to provide the government with situational awareness of cyber threats across critical infrastructure. The statute left it to CISA to fill up the details of the regime, which CISA did in the NPRM.

Under the NPRM, CISA would require "covered entities" – that is, entities in a "critical infrastructure sector" – to report "covered cyber incidents" to the agency. The NPRM's definition of a "covered entity" is quite broad, encompassing all "entit[ies] in a critical infrastructure sector," as defined in Presidential Policy Directive 21. CISA estimates that approximately 316,000 entities will be required to comply with the proposed rule.

The NPRM would require that covered entities report "covered cyber incidents," which it defines as any cyber incident that leads to, among other things, a "substantial loss of confidentiality, integrity or availability of a covered entity's information system or network," a "serious impact on the safety or resiliency of a covered entity's operational systems and processes," a "disruption of a covered entity's ability to engage in business or industrial operations," or "unauthorized access to a covered entity's information system or network." When a covered entity reasonably believes it has experienced a covered cyber incident, the NPRM would require that entity to report the incident within 72 hours. Ransomware payments must be reported within 24 hours. The NPRM would give CISA various tools for compelling enforcement with the reporting regime, including requests for information, subpoenas, acquisition penalties (including debarment) and potential referral of serious cases to DOJ.

The NPRM signals that an accelerated, broadly applicable cyber incident reporting regime is coming to the United States – a regime whose reporting requirements will apply broadly to most large and medium business that operate within a "critical infrastructure sector." The comment period closed on June 3, 2024; a final rule is due by October 2025 and could contain significant updates to reflect priorities of the new administration.

6. Final CMMC program rule kicks off third-party assessment of defense contractor cybersecurity controls

On October 15, 2024, the Department of Defense ("DOD") released a long awaited final rule formalizing its Cyber Maturity Model Certification (CMMC) program. The CMMC was created to strengthen the defense industrial base cybersecurity and better safeguard DOD information, though it aligns with the existing information security requirements for the defense industrial base.

The CMMC model is designed to protect Controlled Unclassified Information ("CUI") and Federal Contract Information ("FCI") shared with defense contractors and subcontractors during contract performance. CUI is "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls." FCI is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, excluding information provided by the Government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments."

Although DOD has long contractually required companies that handle CUI and FCI to abide by certain cybersecurity controls published by the National Institute of Standards & Technology ("NIST"), CMMC mandates that contractors and subcontractors that have CUI obtain third-party assessments and certifications verifying their compliance. The final rule, which took effect on December 16, 2024, allows certified third-party assessment organizations to begin assessing contractor compliance, although there is a phased implementation schedule for the overall program and a separate rule implementing the CMMC contract requirements is not expected until sometime in 2025.

7. Post-*Chevron* cybersecurity regulation

The Supreme Court's 2024 decision in *Loper Bright Enterprises* v. *Raimondo* foreshadows a period of greater judicial scrutiny of federal cybersecurity regulations and caution in agency rulemakings.

Prior to *Loper Bright*, the Court applied a two-step framework set forth in *Chevron U.S.A. Inc.* v. *Natural Resources Defense Council, Inc.*, in which a court would defer to an agency regulation interpreting a statute if (1) the statute was ambiguous and (2)

the agency's interpretation was reasonable. In *Loper Bright*, the Court held that this approach violated the Administrative Procedure Act, and that courts must instead "exercise their independent judgment in deciding whether an agency has acted within its statutory authority," without "defer[ring] to an agency interpretation of the law simply because a statute is ambiguous."

Following *Loper Bright*, federal courts began to consider the decision's framework in national-security and cybersecurity contexts. In *Van Loon* v. *Department of the Treasury*, the U.S. Court of Appeals for the Fifth Circuit struck down a determination by the Office of Foreign Assets Control to sanction Tornado Cash, an open-source blockchain software project used to enhance the privacy of transactions, which North Korean hackers had used to launder money. In reaching this decision, the court relied on *Loper Bright* to conclude that the agency's authority to block "property" in the International Emergency Economic Powers Act to refer to things "capable of being owned" – not immutable, open-source software.

Given the range of cybersecurity regulatory efforts already in progress, agencies will also need to consider *Loper Bright* and will likely attempt to identify more specific legislative authorizations for their actions, in order to guard against litigation challenges. For example, as discussed above CISA is expected to issue a final rule implementing reporting requirements for critical infrastructure entities to report certain incidents and ransomware payments under CIRCIA, and several commenters cited *Loper Bright* during the rulemaking to advocate for further clarity and tailoring in the rule. Similarly, the Transportation Security Administration ("TSA") has issued a notice of proposed rulemaking to impose cyber risk management and reporting requirements on surface transportation owners and operators, relying on its authority under the Implementing Recommendations of the 9/11 Commission Act of 2007 to oversee vulnerability assessments and security plans for certain surface transportation entities.

8. EU update: Cyber Resilience Act, NIS2 implementation, and the Cybersecurity Act

This year has seen a number of significant cybersecurity legislative developments in the EU to bolster its cybersecurity regulatory framework. The EU's latest landmark cybersecurity legislation, the Cyber Resilience Act ("CRA"), was formally adopted on October 10, 2024 and came into force on December 10, 2024. The CRA plugs the "Internet of Things" cybersecurity gaps left by more targeted EU legislation (including the 2023 Data Act) and imposes technical, monitoring, reporting and documentation obligations on manufacturers (and, to a lesser extent, importers, distributors and authorized representatives) of products with digital elements (including hardware and software products and their remote data processing solutions). Fines for non-compliance can reach the higher of €15 million or 2.5% of worldwide annual turnover. The CRA only applies to those businesses to the extent that the same obligations are not covered by other legislation (such as the AI Act), and companies have until December 2027 to meet most of the CRA's requirements (although some manufacturer vulnerability and incident reporting obligations will apply beginning in June 2026).

October 17, 2024 was the deadline for Member States to implement the NIS2 Directive, which requires Member States to legislate for a minimum level of cybersecurity standards amongst operators in certain critical industries, including certain digital infrastructure, business-to-business IT support, and social networking, and search engine and online marketplace service providers. That implementation deadline came and went with limited fanfare given that it was met by only six of the 27 Member States. Although yet to be implemented across most of the EU, the NIS2 Directive promises to shake-up cybersecurity risk management processes for an expanded scope of businesses established in, or providing services into, the EU, including by imposing a 24-hour reporting obligation for significant incidents, enhanced supply chain diligence and cybersecurity risk management requirements, and cybersecurity responsibilities for boards and senior management. In November 2024, the European Commission also adopted additional NIS2 implementing regulations for digital service providers, which raise the bar for reporting security incidents and provide guidance on how to calculate the losses that trigger a notification requirement.

Finally, on December 2, 2024, the European Council approved an amendment to the EU's 2019 Cybersecurity Act. The Cybersecurity Act established a (generally voluntary, although mandatory for certain types of businesses as set out in the Cyber Resilience Act) EU-wide cybersecurity certification scheme, managed by the European Union Agency for Network and Information Security ("ENISA"), for network and information system products and transmission, storage and processing services.

The amendment, which is expected to enter into force in early 2025, will expand that scheme to allow for the certification of managed security services (such as incident handling, penetration testing, security audit and consulting services).

9. GDPR update: Enforcement continues with hundreds of millions in fines

European regulators have continued to actively enforce the GDPR and issue significant fines (calculated on the basis of worldwide annual turnover) against tech companies for breaches involving cross-border transfers, inadequate data security and failures to properly establish lawful bases of processing. These decisions demonstrate not only the ongoing effectiveness of the GDPR's "one-stop shop" regulatory framework, but also the willingness of regulators to levy fines in the absence of any data loss or exfiltration.

On July 22, 2024, the Dutch regulator fined a U.S.-based ride sharing company €290 million for failing, for a period of two years after the EU-US Privacy Shield mechanism was found to be invalid, to maintain adequate safeguards when transferring drivers' personal data (including sensitive data such as medical and criminal records) to the company's servers in the United States. The Dutch regulator led the investigation in its role as the company's lead GDPR supervisory authority after the French regulator shared complaints made on behalf of more than 170 French drivers for the company.

On September 26, 2024, the Irish regulator fined a U.S. technology company €91 million for storing social media users' account passwords without any cryptographic protection or encryption. Although the passwords were never available outside of the company and the company had notified the Irish regulator of its own breach, the regulator nevertheless found that the company had contravened the GDPR's integrity and confidentiality principles (and certain specific regulations) by failing to: (a) use appropriate technical or organizational measures to ensure an appropriate level of security of users' passwords; and (b) promptly notify the regulator of, and document, the breach.

On October 22, 2024, following complaints initially made to the French regulator, the Irish regulator fined a U.S. social media platform €310m for contravening the GDPR principle of lawful, fair and transparent processing. In this case, the company was found to have no lawful basis for processing members' personal data for behavioral advertising and targeted advertising purposes as a result of its failure to obtain valid consent, establish a legitimate interest or demonstrate the contractual necessity of its processing.

10. U.S. state privacy law update: Vigorous enforcement under state causes of action

Looking ahead, 2025 promises to continue the trend of increasing state-level enforcement of comprehensive privacy laws. Comprehensive privacy laws in eight states[1] will take effect over the course of 2025, and states with active comprehensive bills in effect are continuing to refine their enforcement priorities.

For example, the Connecticut Attorney General, which is tasked with enforcing the Connecticut Data Privacy Act ("CTDPA"), has published a report noting its focus on ensuring data rights mechanisms are put in place by covered entities – including data brokers – and in working order. The AG report also emphasizes that covered entities must disclose and obtain adequate consent *prior* to processing teen and sensitive data, which includes biometric information, genetic data, precise geolocation data. Although no enforcement actions were brought in 2024, the Connecticut AG has issued more than a dozen violation notices.

Other states have set up enforcement infrastructure, such as special units within regulators and portals for consumers to escalate complaints. These efforts by regulators signal an increasing focus on privacy violations over other areas where regulators have focused in recent years, including data breaches and other cybersecurity incidents.

[1] The Delaware Personal Data Privacy Act, Iowa Consumer Data Protection Act, Nebraska Data Privacy Act and New Hampshire SB 255 became effective on January 1, 2025; the New Jersey SB 332 becomes effective on January 15, 2025; the Tennessee Information Protection Act takes effect on July 1, 2025; the Minnesota Consumer Data Privacy Act takes effect on July 31, 2025; and the Maryland Online Data Privacy Act takes effect on October 1, 2025.

This prioritization of privacy enforcement can be seen by the recent investigation opened by Texas Attorney General Ken Paxton into car manufacturers' collection and sale of data collected by vehicles. The investigation squarely focuses on the potential privacy violations from such conduct, including the lack of consent for collection of sensitive data. Notably lacking from the scope of the investigation is any discussion of cybersecurity of those connected vehicles – which is an area increasingly being ceded to federal regulators by the states. The September 2024 settlement reached by the Texas AG against Pieces Technology, an AI healthcare company, also made clear that AI companies must disclose the types of data used to train the AI technologies, in addition to disclosures of the likelihood of inaccuracies of the AI outputs in sensitive settings.

Both Texas and California, states that have historically acted as the vanguard of state-level enforcement of privacy laws, have followed the trend of increased regulatory activity in the this space. Beyond its investigation into car manufacturers, described above, the Texas AG's Office has pursued enforcement actions for violation of the Texas's Capture and Use of Biometric Identifier ("CUBI"). On July 30, 2024, the Office announced that it had reached a $1.4 billion settlement related to alleged deployment of facial recognition software in violation of CUBI. Meanwhile, the California AG's Office has entered three stipulated judgments under California state privacy laws in 2024, including a $375,000 judgment for allegedly selling the personal data of California residents without providing notice or the opportunity to opt out, in violation of the California Consumer Privacy Act and California Online Privacy Protection Act.

As the next wave of state privacy laws comes into effect, and state regulators beef up efforts to enforce existing obligations, companies should ensure they are monitoring and assessing their compliance obligations under each state law.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

John Patten
+44-20-7367-1684
jpatten@paulweiss.com

Alex Zapalowski
+44-20-7367-1697
azapalowski@paulweiss.com

Associates Charlie Burrell, Neil Chitrao, Matthew J. Disler, Uche Eseonu, Rachel Gallagher, Corey Goldstein and Cole A. Rabinowitz contributed to this Client Memorandum.