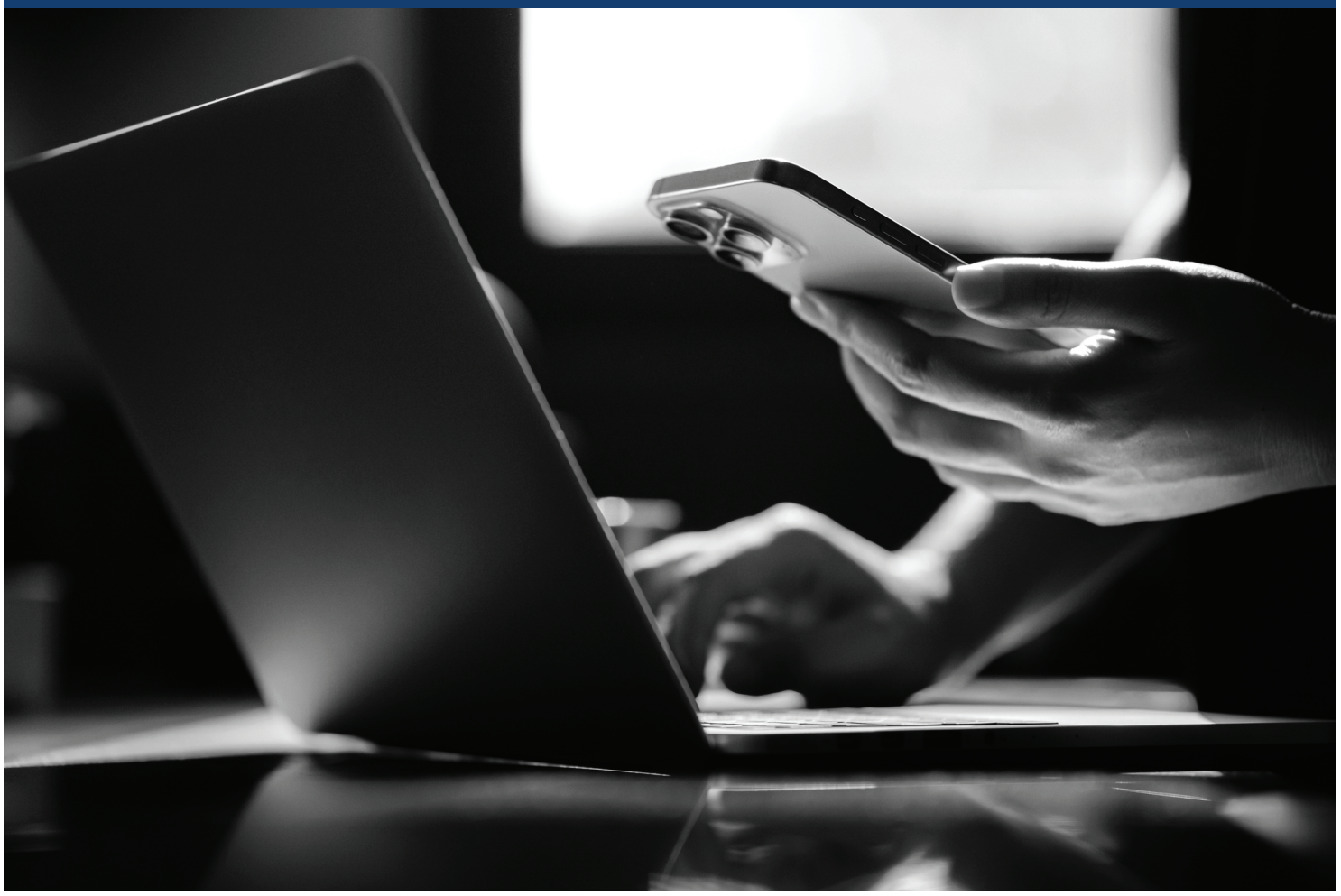
Paul, Weiss

2025 Year in Review

Cybersecurity and Data Protection



Paul, Weiss

Client Memorandum

January 7, 2026

2025 Year in Review: Cybersecurity and Data Protection

Key Topics

Executive Summary	1
State and Federal Cyber Regulatory Updates	3
Developments in State Data Privacy Laws	6
Updates to International Privacy and Cyber Regulations	8
Trends in Threat Actor Activity and Law Enforcement Response	10
Enforcement	12
Privacy and Cyber Litigation	17

Executive Summary

Cybersecurity and data privacy issues posed challenges and opportunities for growth for businesses in 2025. Cutting across industries, companies contended with the threat of ransomware and other cyber attacks, social engineering schemes, and the consequences of sophisticated supply chain attacks against vendors, as threat actors leveraged artificial intelligence ("AI") to increase their scale and sophistication.

Global regulators imposed novel cybersecurity and privacy obligations, with a particular focus on requirements for enhanced cybersecurity infrastructure, data subject notice and consent, and the protection of data deemed "sensitive." In the United States, federal and state regulators introduced new private sector cyber and privacy requirements, including a novel national security regime regulating the overseas transfer of U.S. sensitive personal data. Enforcement actions under state privacy laws continued to increase in frequency and settlement size. Internationally, jurisdictions including the European Union, United Kingdom, China and India implemented new privacy and data security obligations for companies operating within their borders.

Below, we survey the year 2025's most consequential developments in cybersecurity and data protection and offer practical considerations for compliance strategy, incident readiness and vendor governance. In light of these changes, in the data privacy space we expect to see more mandatory reporting, tighter vendor oversight and stronger consumer-privacy rules—within the cyber security sphere we anticipate continued pressure on state-sponsored actors and more litigation around biometrics and web-tracking.

2025 at a Glance

Regulators, courts and threat actors moved fast over the past year. On the enforcement side, the Department of Justice ("DOJ") implemented new regulations limiting the transmission of certain "sensitive" U.S. person data abroad, the Securities and Exchange Commission ("SEC") strengthened breach-response and notice duties for certain financial firms, states jockeyed for a leading role in regulatory enforcement, the Cybersecurity and Infrastructure Security Agency ("CISA") delayed its nationwide incident-reporting rule, California updated cybersecurity audit requirements and the European Union put new financial-sector resilience rules into effect. Meanwhile, threat actors also remained busy, with AI-driven social engineering and supply-chain compromises driving incidents in 2025 to record numbers at significant cost to businesses and individuals.

You Should Know

- **Broad data transfer restrictions.** DOJ's new Data Security Program limits transfers of certain quantities of "sensitive" American data to specified countries, creating immediate compliance exposure.
- **Increased burden on financial firms**. The SEC's Regulation S-P now requires written cyber-related policies and procedures, notice to individuals within 30 days absent a "no-harm" finding, increased recordkeeping, and stringent new third-party risk management requirements.
- **Escalating threat from nation state actors.** 2025 was a record-breaking year for threat actors across geographies and levels of sophistication. Despite law enforcement action against actors linked to China and North Korea, attacks involving AI, supply-chain compromises and social engineering cost billions across industries.

Where to Focus in 2026

Looking ahead, cyber-related risk can be mitigated by prioritizing cross-border data mapping, taking steps to ensure incident-reporting readiness, enhancing vendor governance policies and aligning consumer information policies with relevant regulatory requirements. Here are a few areas we are keeping an eye on in 2026:

- **Critical infrastructure reporting requirements**. CISA delayed the implementation of new incident reporting requirements to an expected date of May 2026, leaving state-specific reporting rules to govern the space. Voluntary federal reporting continues, with increased government engagement often proving helpful to impacted businesses.
- **Increased risk of AI-assisted cyber attacks.** Trends reveal the escalating use of cheap and readily accessible AI tools by threat actors to effectuate cyber attacks as well as to find unpatched or zero-day vulnerabilities. These tools will continue to allow threat actors to increase the scale and speed of their attacks across industries.
- **Cybersecurity audit requirements and third-party scrutiny.** California continued to implement novel regulatory requirements, including new audit mandates and rules for risk assessments. These requirements started to phase in on January 1, 2026.
- **New AI cybersecurity guidelines on the horizon.** In late 2025, the National Institute of Standards and Technology ("NIST") released an initial draft of new guidelines for how businesses should orient their cybersecurity programs to safely integrate the use of AI. We expect these guidelines will be finalized in 2026.

State and Federal Cyber Regulatory Updates

DOJ Data Security Program Takes Effect

DOJ's Data Security Program ("DSP")—commonly referred to as the bulk data rule—was issued on January 8, 2025, and quickly became effective with staggered effective dates of April 8 and October 6, 2025.[1] The DSP is a significant new regulatory regime for data security with the potential to impact the operations of companies engaged in international business.

The DSP prohibits or restricts the provision of U.S. bulk "sensitive" personal data (such as certain personal identifiers, biometric and health data) and U.S. government-related data to "countries of concern" (including China, Russia or Iran). In practical terms, according to DOJ, "individuals and entities subject to U.S. jurisdiction, as well as foreign individuals and entities conducting business in or with the United States or with U.S. persons, must comply with the Data Security Program."[2] Unlike conventional data privacy regulations emphasizing consumer protection, the DSP's purpose is to protect U.S. national security, and individuals cannot consent to waive the DPS's requirements. Companies that obtain, process or transfer data as part of their operations should evaluate how the DSP may apply to their business and consider adjusting their compliance programs and relationships accordingly.

You Should Know

- **Broad scope.** The DSP covers multiple defined categories of "sensitive" personal data and applies to a wide range of counterparties and otherwise routine cross-border commercial arrangements. The regulated transaction types are broad, including data brokerage, vendor, employment, and investment agreements.
- **Substantive restrictions.** The DSP regulates transfers of U.S. person bulk sensitive personal data and U.S. government-related data to countries of concern and their covered persons, and permits certain categories of "restricted" transactions only if stringent security, due diligence, recordkeeping, and audit requirements are also satisfied.
- **Real penalties**. The DSP is backed by significant civil and potential criminal penalties, calculated on a per transaction basis, including civil fines of up to twice the value of the transaction, criminal fines of up to $1 million or twice the gross gain from the transaction, and prison sentences of up to 20 years.[3]
- **Guidance gaps heighten compliance risk.** DOJ has not yet implemented a process for obtaining licenses or advisory opinions, creating uncertainty as companies calibrate their compliance programs. Industry members must currently rely solely on examples within the final rule which highlighted areas DOJ expected to clarify through future guidance.

Taken together, the fast-tracked effective date and the DSP's breadth across data categories, counterparties, and transaction types represent an aggressive new approach to governing international transfers of sensitive information and government-related datasets outside of the U.S. Companies engaged in cross-border data transfers, which should carefully map their data flows in order to mitigate the risk imposed by this novel and developing legal regime.

CISA Extends CIRCIA Deadline

In April 2024, CISA published a Notice of Proposed Rulemaking ("NPRM") implementing new regulatory reporting mandates imposed by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA").[4] Although CISA was originally expected to publish a final rule in October 2025, a regulatory notice published in Spring 2025 indicated that CISA pushed the expected publication date back to May 2026.[5]

CIRCIA established a mandatory nationwide cyber incident and ransomware payment reporting regime for "covered entities" operating in critical infrastructure sectors. Once effective, CIRCIA would require such "covered entities" to report a "covered cyber incident" within 72 hours, and any ransomware payment within 24 hours.[6]

---

[1] 28 C.F.R. Part 202, available here; Paul, Weiss, *DOJ Issues Final Rule Restricting the Transfer of Certain Sensitive U.S.-Person Data* (Jan. 17, 2025), available here.

[2] U.S. Dep't of Justice, *Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries* (Apr. 11, 2025), available here.

[3] 28 C.F.R. § 202.1301, available here.

[4] *See* Paul, Weiss, *CISA Issues Highly Anticipated, Far-Reaching Rules for Cyber Incident Reporting* (Apr. 3, 2024), available here.

[5] Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements, 1670-AA04, Off. of Info. and Reg. Aff., available here.

[6] *See Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),* CISA, available here (accessed Dec. 8, 2025).

You Should Know

- **Not yet mandatory.** CISA has reiterated that CIRCIA's reporting regime will not be mandatory until a final rule becomes effective.[7] In the interim, the agency has continued to encourage voluntary cyber reporting and has prioritized stakeholder engagement, including discussions of how best to standardize reporting of cyber incidents to the federal government through the DHS-led Cyber Incident Reporting Council.
- **Why the pause matters.** The absence of a final rule preserves the current regulations, in which sector-specific and state reporting obligations continue to drive timelines and notice content.
- **What to do now.** Companies should maintain readiness aligned to the NPRM's structure. CISA urges voluntary reporting of unusual cyber activity or incidents to enable assistance, trend analysis and timely warnings to other potential victims.[8]

Cybersecurity Information Sharing Act of 2015 ("CISA 2015") Extended to January 30, 2026

CISA 2015 was enacted to catalyze the sharing of cyber threat indicators and defensive measures between the federal government and the private sector. The statute provides private parties insulation from liability, antitrust suits and disclosure risks to incentivize such sharing at scale. While Congress allowed the core authorizations underpinning the CISA 2015'sinformation-sharing framework to sunset on September 30, 2025,[9] it temporarily extended CISA 2015 through January 30, 2026, as part of the November 2025 government funding bill. However, without a clear plan for further reauthorization, it remains unclear if its provisions will apply beyond the end of January. While some mechanisms still exist to facilitate private sector reporting of indicators to the government, the statutory incentives that made such sharing attractive—liability protections, antitrust clarity and exemptions from federal and state disclosure obligations—may be weaker now that November 2025 has passed.

You Should Know

- **Potential for reduced visibility.** Given the current uncertainty surrounding CISA 2015, companies may be reluctant to share cyber-threat information going forward, which could result in fewer warnings for peers and less visibility for the government into fast-moving attacks. In its absence, the government may be forced to rely more heavily on post-hoc incident reporting regimes, such as those anticipated to be forthcoming within CIRCIA.
- **Modernization gap.** If not reauthorized, the distance between the CISA 2015's scope and the modern cyber threat landscape would widen, which could be marked by increased targeting of operational technology and edge devices and the rise of AI-enabled attack and defense.
- **What to expect next.** Absent the reauthorization of CISA 2015 in January, the broader cybersecurity ecosystem is unlikely to sustain the pre-sunset pace and breadth of threat intelligence sharing. Businesses should anticipate a continued emphasis on incident reporting and sector-specific directives, alongside efforts to sustain voluntary technical exchanges, including those described in connection with CIRCIA.

Department of Health and Human Services Issues NPRM Under HIPAA

In January 2025, the U.S. Department of Health and Human Services Office for Civil Rights ("OCR") published an NPRM to improve the protections for electronically stored protected health information ("ePHI") in the Health Insurance Portability and Accountability Act ("HIPAA") Security Rule.[10]

Since 2003, the HIPAA Security Rule has established the standards to protect ePHI when a covered entity or business (such as a healthcare provider) creates, receives, transmits or maintains ePHI. The HIPAA Security Rule requires that covered entities implement appropriate physical and technical safeguards to ensure the confidentiality, integrity and security of the ePHI. The rule proposed in January 2025 would significantly enhance existing cybersecurity requirements in response to a challenging cybersecurity threat landscape for healthcare providers.

[7] *See Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),* CISA, available here.

[8] *See Sharing Cyber Event Information: Observe, Act, Report*, CISA (Apr. 2022), available here.

[9] *See* Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1501 *et seq.*

[10] 45 C.F.R. §§ 160, 164, available here.

You Should Know

- **Additional detail regarding mandatory risk analyses**. Under the proposed rule, regulated entities would be subject to more specific requirements regarding the data security measures they take under the HIPAA Security Rule, including the need to create a written assessment that contains, among other things, a review of the technology asset inventory; an identification of all reasonably anticipated threats to the confidentiality, integrity and availability of ePHI and an assessment of the risk level for each identified threat and vulnerability.

- **New annual compliance audit requirements**. Regulated entities would be required to conduct a compliance audit at least once every 12 months to ensure their compliance with HIPAA Security Rule requirements.

- **Additional requirements regarding technical data security measures.** Regulated entities would be required to encrypt ePHI at rest and in transit, with limited exceptions.

Although HHS sought comments on the proposed rule by March 2025, no final rule has yet been published, and industry groups have criticized the proposed rule as impractical and unduly burdensome, while acknowledging the need for updated cybersecurity requirements.[11] The healthcare cybersecurity policy debate around the proposed revisions to the HIPAA Security Rule is set to continue into 2026, and health delivery organizations and businesses in adjacent sectors should stay abreast of those developments as any new policy in this space is likely to raise expectations for businesses and network defenders.

SEC Implements Cyber and Data Protection Requirements Under Regulation S-P

The year 2025 also saw new cybersecurity requirements take effect for a range of SEC-regulated businesses through amendments to the SEC's Regulation S-P ("Reg S-P").[12] Reg S-P applies to broker-dealers, investment companies, SEC-registered investment advisers, funding portals and all transfer agents (including those registered with other banking agencies). Larger entities must comply by December 3, 2025, and all other covered institutions must comply by June 3, 2026. [13]

You Should Know

- **Written policy requirements.** The amendments to Reg S-P require written policies and procedures reasonably designed to detect, respond to and recover from unauthorized access to or use of customer information.

- **Focus on customer notification.** Reg S-P now requires that, absent a documented "no-harm" determination after a reasonable investigation, the covered institution must provide clear and conspicuous written notice to affected individuals as soon as practicable and no later than 30 days after becoming aware of an incident, subject only to limited delays that must be authorized by the Attorney General.

- **Novel recordkeeping obligations.** The amendments to Reg S-P enhanced recordkeeping requirements that demonstrate the implementation of risk assessments, containment and control steps, notice determinations (including any decision not to notify) and data disposal practices. The amendments also broaden the scope of protected data to "customer information," covering both a covered institution's own customers and customers of other financial institutions whose information it receives.

- **New Third-Party Risk Management Requirements.** Covered institutions must now ensure service providers implement appropriate measures to protect customer information, and also provide notice to the covered institution as soon as possible and no later than 72 hours after becoming aware of a breach in a customer information system, after which the institution must promptly initiate its incident response program.

NYDFS Issues New Cybersecurity Requirements and Associated Guidance

In November 2025, amendments to New York Department of Financial Services ("NYDFS") Part 500 took effect with enhanced requirements for data security for nearly all covered financial services entities, including multifactor authentication ("MFA"), asset inventory and data retention.

[11] *See* Dark Reading, *Industry Continues to Push Back on HIPAA Security Rule Overhaul* (Dec. 23, 2025), available here.

[12] *See* 17 C.F.R. § 248.30, available here.

[13] *See* Final Rule, 89 Fed. Reg. 47723 available here.

You Should Know

- **Emphasis on MFA.** NYDFS now requires MFA for virtually all remote access to information systems, expanding the requirement from internal networks to other third-party applications, including cloud applications.
- **New requirements regarding asset inventory.** The amendments also require a comprehensive, documented asset-inventory program. The program must be maintained and validated on a defined cadence, and must include secure data-disposal mechanisms.
- **Focus on third-party risk management.** These operational changes align with NYDFS's recent guidance emphasizing board-level oversight and non-delegable responsibility for third-party cyber risk. Covered entities should identity programs and governance processes and consider measures to ensure these controls are reflected in 2026 annual certifications and embedded in vendor contracts.

In addition to the Part 500 amendments, NYDFS published an cybersecurity advisory aimed at assisting industry in managing risks related to third-party service providers.[14] The advisory highlights potential risks relating to the use of third-party services providers for cloud computing, file transfer systems, AI, and fintech solutions. The guidance emphasizes the importance of active engagement by an organization's leadership to oversee third-party cyber risk, including annual review and approval of the organization's cybersecurity policies.

CalPrivacy Introduces New Cybersecurity Requirements Pursuant to CCPA

In July 2025, CalPrivacy (formerly named the California Privacy Protection Agency) adopted new requirements for cybersecurity audits pursuant to the California Consumer Privacy Act ("CCPA"). These new regulations require annual, independent cybersecurity audits covering the core components of a business' cybersecurity programs.

As described below, based on whether the business poses a significant risk to consumers' privacy and based on the business' annual revenue, the cybersecurity audit requirement becomes effective starting April 1, 2028, with further effective dates staggered to April 1, 2029 and April 1, 2030 based on revenue.[15]

Developments in State Data Privacy Laws

In the absence of comprehensive federal privacy legislation, the number of states with comprehensive privacy laws in effect nearly doubled from nine states in 2024 to 16 in 2025. Another three states have already enacted laws that will go into effect in 2026. And roughly half of states with existing privacy laws amended those laws in 2025 to change applicability thresholds, with most broadening their laws' applicability to include more businesses.

Protection of Minors Has Been an Emphasis in State Privacy Lawmaking

A key area of focus for states in 2025 involved enhancing protections for minors. Lawmakers in at least 10 states passed new laws or amended existing laws or regulations to implement stronger protections around the processing of children's personal data, including through amendments to general consumer privacy statutes and enaction of new Age-Appropriate Design Codes ("AADCs").

You Should Know

- **AADCs in a nutshell.** AADCs are design-centric laws emphasizing an organization's duty to build online products and services with safeguards tailored to protect children's privacy and safety, typically through privacy-protective defaults and limits on features that could expose minors to risks.
- **AADC developments this year.** New AADC-style laws were enacted in Nebraska and Vermont in 2025. While both laws incorporate requirements that restrict, for example, communication with minor accounts by unconnected users, Vermont's Appropriate Design Code Act goes further by establishing a duty of care to protect minors in the design of online products.[16] Nebraska's law, unlike most other AADCs that focus primarily on tools for use by minors, also includes mandatory tools for parents to monitor and limit a child's use of online services.[17]

[14] New York Dep't of Financial Services, *Guidance on Managing Risks Related to Third-Party Service Providers* (Oct. 21, 2025), available here.

[15] California Privacy Protection Agency, *California Finalizes Regulations to Strengthen Consumers' Privacy* (Sept. 23, 2025), available here.

[16] Nine Vt. Stat. Ann. Pt. 3, Ch. 62, Subch. 6 § 2449f.

[17] 2025 Nebraska L.B. 504 (2025).

- **New protections for minors beyond AADCs.** Separately, states also advanced protections for minors through updates to general consumer privacy statutes and regulations. California and Connecticut, for example, amended existing privacy statutes and regulations to expand the definition of "sensitive data" to capture personal information of consumers under 16 to the extent that a business has actual knowledge of that consumer's age.[18]

Updated California Regulations Set New Baseline for Consumer Privacy Protection

California rolled out long-anticipated regulations in 2025 that impact businesses' data privacy obligations. On July 24, 2025, after years of hearings and comment periods, CalPrivacy adopted new regulations under the CCPA that included not just the cybersecurity audits discussed above, but also new rules for risk assessments and automated decision-making technology ("ADMT"), as well as updates to existing CCPA regulations.[19]

You Should Know

- **Plan now for sequencing, scoping, and vendor flow-downs**. In light of the CCPA requirements coming into effect in 2026 and 2027, businesses should consider creating an inventory of ADMT use cases and "significant risk" processing, develop CCPA-compliant risk-assessment programs and update notices, rights workflows, and privacy policies. Businesses should also consider whether contracts and technical controls are aligned so service providers support opt-outs, data access/portability and ADMT transparency obligations.

- **Independent cybersecurity audits begin in 2028**. Annual independent cybersecurity audits will apply to businesses if their processing of personal data poses a "significant risk" to consumer security, defined to include businesses that process a majority of their business from selling or sharing personal data, and businesses that had more than $26.625 million in revenue in the preceding year and either processed the personal data of more than 250,000 California residents or the sensitive personal data of more than 50,000 California residents. The compliance dates for the audits are staggered by revenue and are early as April 1, 2028.

Risk Assessments

The new risk assessment regulations, which go into effect for businesses currently processing consumer personal information on December 31, 2027, require businesses to conduct and maintain risk assessments prior to initiating processing activities that pose a "significant risk" to consumer privacy. Activities can involve a "significant risk" to consumers' privacy when they relate to the selling, sharing, profiling or processing of a consumer's personal information.

The regulations state the goal of the risk assessments is to restrict or prohibit "the processing of personal information if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public."[20] The risk assessments requirements are comprehensive to evaluate potential "negative impacts" to consumers and ensure stakeholders' involvement so all employees' risk assessment processing duties are thoroughly accessed.

Risk assessments will be required every three years, unless a business makes a material change relating to a processing activity. If so, the business will have 45 days to perform and submit a risk assessment to CalPrivacy. The regulations allow businesses to conduct and maintain their own comparable risk assessments as long as those risk assessments contain the information required within the regulations.

ADMT Restrictions

CalPrivacy introduced ADMT restrictions to the CCPA regulations, defining ADMT as "any technology that processes personal information and uses computation to replace human decision-making or substantially replace human decisionmaking."[21] However, the CCPA narrowly regulates the use of ADMT, including decisions that affect "finances, housing, education, employment or health care," but excluding decisions related to advertising.[22]

[18] Cal. Civ. Code § 1798.99.30 (California); C.G.S. § 25-113 (2025).

[19] California Privacy Protection Agency, *CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Regulations* (Sep. 23, 2025), available here.

[20] Cal. Admin. Code tit. 11 § 7154.

[21] *Id.* at § 7001(e).

[22] *Id.* at § 7001(ddd).

Beginning on January 1, 2027, when a business uses ADMT, the regulations require that consumers be provided with pre-use notice, opt-out of use requests, and requests to access the ADMT's output of their personal information.

Updates to Existing CCPA Regulations

In addition to the new cybersecurity audits, risk assessments and ADMT regulations, several existing CCPA regulations were updated. Beginning on January 1, 2026, all the existing updated CCPA regulations become effective. Businesses will be required to provide consumers the personal information collected prior to the 12-month period preceding the business's receipt of the consumer's request. However, the regulations only require businesses to provide past personal information, with a backstop date of January 1, 2022, or later, as long as it is not impossible and does not create a disproportionate burden.

Another change is the expansion of the definition of sensitive personal information to include consumer personal information unless that business has actual knowledge that consumers are less than 16 years of age, clarifying "[a] business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age." The updates to the CCPA regulations require covered businesses to impose non-discriminatory language in CCPA their privacy policies, to make clear that consumers have the right "not to be retaliated against for exercising privacy rights conferred by the CCPA, including when a consumer is an applicant to an educational program, a job applicant, a student, an employee, or an independent contractor."

Updates to International Privacy and Cyber Regulations

Significant developments to the cyber and privacy regimes have not extended beyond the United States. Across the world, regulators have imposed novel requirements to both protect privacy rights and enhance private sector cybersecurity measures.

The EU remains the global benchmark through the General Data Protection Regulation ("GDPR"). This section highlights global privacy and data protection trends, beginning with the EU/UK, before shifting focus to privacy developments in China and India to illustrate broader trends.

European Union and United Kingdom: Cybersecurity Developments

The European Union and the United Kingdom implemented a number of significant updates to cybersecurity regulations in 2025. Most notably, the EU's Digital Operational Resilience Act ("DORA") went live across the bloc in January 2025, substantially tightening cybersecurity requirements for the financial services sector and critical IT service providers that are based in or provide services into the EU.[23]

You Should Know

- **DORA is enforceable now**. As of January 17, 2025, institutions and critical IT providers operating in the European Union face prescriptive mandates about incident reporting, resilience testing, and third-party oversight, with member state penalties that can be significant. Programs, vendor contracts, and testing calendars should consider alignment with DORA's operational detail.

- **NIS2 obligations currently vary by country**. Uneven uptake across EU member countries has resulted in varying industry coverage, differing reporting timelines and differing penalty frameworks. Entities should consider mapping in-scope operations and aligning controls to the most stringent applicable member state rules while monitoring for further European Commission and national action.

- **United Kingdom is moving toward DORA/NIS2-style rules**. The United Kingdom's Cyber Security and Resilience Bill will likely expand the Network and Information Security ("NIS") regime to more entities, tighten incident reporting, and impose obligations on designated critical suppliers regardless of corporate domicile. U.K.-facing organizations should assess potential in-scope services and supply chain exposure.

DORA imposes detailed obligations in areas including IT security, incident reporting, resilience testing and oversight of critical vendors, and is designed to force organizations to take a more proactive approach to IT risk management. Penalties for noncompliance are generally determined at a member state level, with the Italian regulator currently having the right to impose the largest fines for non-compliance (up to €20 million).

In addition , the European Union's Network and Information Security Directive ("NIS2")—designed to create a single cybersecurity framework across an expanded scope of critical sectors—is still running into implementation headwinds despite

[23] EUR-Lex, Document 32022R2554, PE/41/2022/INIT, available here.

its October 2024 transposition deadline.[24] Only 15 of 27 EU member states have fully transposed the rules into national law, despite the European Commission in May 2025 issuing reasoned opinions to 19 Member States for having failed to do so (though the European Commission is yet to take any further action).[25]

In February 2025, the first certification scheme for IT service providers under the European Union's Cybersecurity Act became available, based on the Common Criteria international standard.[26] The scheme provides a voluntary mechanism for IT service providers to obtain proof of assurance through certification of its products according to their level of cybersecurity throughout their lifecycle. In addition, in June 2025, the European Union Agency for Cyber Security launched a process to develop a candidate certification scheme for managed security services.[27]

Finally, the United Kingdom has taken steps of its own to enhance cybersecurity practices for essential digital services by introducing to Parliament the long-awaited Cyber Security and Resilience Bill in November 2025, taking inspiration from DORA and NIS2.[28] The bill seeks to expand the UK's existing Network and Information Security framework to apply to an expanded range of entities (including data centers and electricity load controllers), while adopting broader regulatory powers to investigate potential vulnerabilities, and imposing tighter incident-reporting requirements. Similar to DORA, the bill also imposes obligations on certain designated "critical suppliers" with a view to fortifying supply chains. The bill remains in early stages of its passage through Parliament and should be monitored on its legislative journey through 2026.

European Union and United Kingdom: Data Privacy Developments

Big ticket GDPR regulatory enforcement by European regulators continued in 2025, with significant fines (calculated on the basis of worldwide annual turnover) against tech companies for breaches involving cross-border transfers, transparency and consent to direct marketing activities. In May 2025, the Irish Data Protection Commission issued a fine against TikTok for €530 million for unlawful transfers of European Economic Area ("EEA") user data to China, citing TikTok's failure to verify, guarantee and demonstrate that personal data of EEA users was afforded a level of protection equivalent to that guaranteed in the European Union, and had not adequately informed users about the nature of the transfers.[29] Furthermore, in September 2025, the French national data privacy regulatory agency fined Google €325 million for displaying advertisements in Gmail's "Promotions" and "Social" tabs without valid user consent, and for deploying advertising cookies during account creation in a manner that distorted user choice.[30]

In more positive news for American businesses, in September 2025, the European General Court dismissed a challenge brought by a Member of the French Parliament, Philippe Latombe**,** against the European Commission's adequacy decision for the EU-U.S. Data Privacy Framework ("DPF") (on which more than 3,400 U.S. companies rely for transatlantic data flows).[31] Latombe's arguments included that the DPF lacked independent judicial oversight, in violation of the EU Charter of Fundamental Rights and the GDPR, and failed to provide sufficient safeguards against bulk data collection. The General Court upheld the validity of the DPF, finding that the European Commission had adequately assessed the protections in place at the time of its decision, whilst noting the European Commission's role in continuously monitoring the DPF's validity. Businesses with U.S. operations welcomed that the decision had not gone the same way as the EU-U.S. Safe Harbor and EU-U.S. Privacy Shield under the 2015 and 2020 Schrems judgments.

In June 2025, the United Kingdom's long-awaited GDPR reforms received royal assent through the Data (Use and Access) Act 2025. The Act seeks to modernize the U.K.'s data protection regime and provide a boost to business and innovation, while still upholding the principles of the U.K. GDPR.[32]

---

[24] Paul, Weiss, *Year in Focus: Key Cybersecurity and Privacy Developments in 2024* (Jan. 21, 2025), available here.

[25] European Commission, *Commission calls on 19 Member states to fully transpose the NIS2 Directive* (May 7, 2025), available here.

[26] European Union Agency for Cybersecurity, *EUCC Certification Scheme* (last accessed Dec. 21, 2025), available here.

[27] European Union Agency for Cybersecurity, *EU Managed Security Services Certification to drive the cybersecurity market* (June 25, 2025), available here.

[28] UK Government, *Cyber Security and Resilience Bill* (Nov. 18, 2025), available here.

[29] Irish Data Protection Commission, *Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China* (May 2, 2025), available here.

[30] Commission Nationale de l'Informatique et des Libertés, *Cookies and advertisements inserted between emails: Google fined 325 million euros by the CNIL* (Sept. 3, 2025), available here.

[31] EUR-Lex, Document 62023TJ0553, Case T-553/23 (Sept. 3, 2025), available here.

[32] The National Archives, *Data (Use and Access) Act 2025* (June 19, 2025), available here.

The Act marks the United Kingdom's first express divergence from the EU GDPR. Among other things, relative to the GDPR, the Act reduces obligations relating to automated decision-making, legitimate interests, data subject accesses requests and cookies. The Act also increases penalties for breaches of the U.K.'s E-privacy legislation (Privacy and Electronic Communications Regulations (EC Directive) 2003) to align with penalties set out in the U.K. GDPR.[33] The draft decision is currently undergoing review by the EU Member States.

India and China

China's Network Data Security Management Resolutions and India's Digital Personal Data Protection Act ("DPDPA") are reflective of an increasingly global commitment to safeguarding individual rights to data privacy, including the right to consent to personal data processing.

On January 1, 2025, the Network Data Security Management Regulations, released in September 2024, came into effect, strengthening network data governance alongside other data security and privacy laws.[34] The Regulations impose tighter personal data requirements—including detailed privacy-policy content and display rules (a dual-list for collection and third-party sharing), separate consents where required and obligations to respond to data-portability requests.[35] The Regulations also require annual and scenario-based risk assessments and safeguards for important data, and make network platform service providers responsible for defining third-party security obligations and liable for supervisory failures.

The DPDPA establishes a consent-based framework to regulate the processing of all digital personal data (data collected in digital form, or later digitized) of India's residents.[36] It demands "free, specific, informed, unconditional and unambiguous" consent from individuals before processing their personal data. Consent must be an affirmative act; pre-checked boxes or implied agreements are prohibited.[37] In 2025, the Ministry of Electronics and Information Technology ("MeitY") released the Draft Digital Personal Data Protection Rules (the "Draft Rules"), 2025 for public consultation,[38] which includes operational aspects such as consent notices, registration and obligations of consent managers, breach notification, children's data, grievance mechanisms and the Data Protection Board of India's obligations.[39] The Draft Rules have not taken effect.

Trends in Threat Actor Activity and Law Enforcement Response

You Should Know

- **AI is amplifying attacker scale and speed**. Threat actor campaigns are increasingly using AI to automate reconnaissance, phishing, and exploitation at scale. Regulators and counterparties will likely scrutinize whether enterprises log AI usage, enforce least-privilege access and maintain phishing-resistant authentication and timely patching.
- **Identity-focused intrusions are surging**. Threat actors are increasingly pivoting from perimeter exploits to social engineering and identity abuse—targeting multifactor authentication, employee-facing help desks and user access consents—to obtain and exploit elevated access in SaaS environments.
- **Extortion remains the business model of choice.** Data theft followed by pressure-based extortion, including some level of encryption, continues across sectors. Preparedness measures include credential hygiene, SaaS application governance and tested response protocols that assume identity compromise.

Trends in Threat Actor Activity

1. Social Engineering-Enabled Data Theft and Cyber Extortion. Threat actors continued to pursue data theft and cyber extortion in 2025, often in new groupings of bad actors. A combined group of actors from three previously distinct threat actor groups—Scattered Spider, ShinyHunters and LAPSUS$—collectively claimed responsibility for a series of significant breaches

[33] Paul, Weiss, *The UK's Data Protection Reforms Finally Arrive: What you Should Know About the Data (Use and Access) Act* (June 23, 2025), available here.

[34] Barbara Li, *China issues the Regulations on Network Data Security Management: What's important to know* (Oct 16, 2024), available here.

[35] *Id*.

[36] Aakanksha Tewari, *India's Digital Personal Data Protection Act (DPDPA)*, available here.

[37] *Id*.

[38] Ministry of Electronics and Information Technology, *MeitY releases Draft Digital Personal Data Protection Rules, 2025 for public consultation; Feedback/comments sought from public by 18th February, 2025, PIB Delhi* (Jan. 3, 2025), available here.

[39] *Id*.

associated with Salesforce customer environments throughout the year.[40] In the Salesforce-related incidents, companies saw their employees targeted by social engineering attacks, in which they were deceived into providing credentials or authorizing a malicious application in their company's Salesforce instance. The threat actors then used those credentials to steal customer data.[41]

2. Supply Chain Attacks. Supply chain compromises intensified in both scale and sophistication in 2025, driven notably by the increasing use of AI by attackers and a strategic pivot toward the digital backbone that connects enterprises. Throughout the year there was a continued surge in third-party and hosted-service compromises across cloud and SaaS ecosystems where attackers leveraged vendor access and multi-tenant architectures to move laterally, harvest credentials and exfiltrate data across downstream customers. Compared to direct compromises, third-party breaches had higher average costs and longer detection and containment windows.

Adversaries also sustained a targeted focus on core digital infrastructure and service providers. Government and industry reporting highlighted China-nexus campaigns such as Salt Typhoon (which infiltrated major telecommunications networks worldwide for long-term espionage)[42] and Volt Typhoon (which prepositioned capabilities within critical infrastructure environments), underscoring the systemic risk when backbone routing, edge devices and authentication pathways are compromised.[43]

Incidents involving the private sector illustrate these themes. Oracle Health disclosed a January 2025 incident tied to legacy servers not yet migrated to Oracle Cloud,[44] while a separate July 2025 Oracle breach triggered litigation over the exposure of extensive personal and financial data for employees and contractors of enterprise customers.[45] Red Hat reported unauthorized access to a consulting GitLab instance, with copied engagement materials but no identified impact to its product software supply chain.[46]

3. AI-Enabled Cyberattacks. This year has also seen an increase in the use of AI capabilities to launch cyberattacks. In a November 2025 report, Anthropic described its disruption of what it characterized as the first publicly reported AI-orchestrated cyber-espionage campaign.[47] The campaign, initiated by a PRC sponsored group called GTG-1002, leveraged the AI platform Claude Code to execute roughly 80% to 90% of the operations of the campaign autonomously.[48] The GTG-1002 campaign will also likely lead to regulatory attention to dual-use AI, including expectations for providers to detect and throttle automated abuse, and for enterprises to govern employee use of AI tools consistent with privacy, data protection and sectoral obligations.

Law Enforcement Activity

DOJ continued to focus enforcement on apprehending threat actors and recovering funds obtained through cybercrime.

Significant federal law enforcement actions targeted threat actors affiliated with nation-states, particularly actors affiliated with the People's Republic of China ("PRC"). For example, in January 2025, the Office of Foreign Assets Control announced sanctions against Sichuan Juxinhe Network Technology Co., Ltd., a cybersecurity firm that was affiliated with the Salt Typhoon state-sponsored threat actor group, which was reported to be responsible for several intrusions into U.S. telecommunications infrastructure.[49] In August 2025, CISA, the NSA and more than a dozen international agencies issued a joint cybersecurity advisory describing techniques used by Salt Typhoon actors.[50] Also consistent with this focus, in July 2025,

[40] Krebs on Security, *ShinyHunters Wage Broad Corporate Extortion Spree* (Oct. 7, 2025), available here.

[41] Google Threat Intelligence Group, *The Cost of a Call: From Voice Phishing to Data Extortion* (June 4, 2024), available here; Wall Street Journal, *Salesforce-Linked Security Breach Fallout Escalates With Qantas Leak* (Oct. 15, 2025), available here.

[42] Congress, *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications* (Jan. 23, 2025), available here.

[43] CISA, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure* (Feb. 7, 2024), available here.

[44] Brian Rankin, *Oracle Health Breach: What Life Sciences Cybersecurity Leaders Need to Know—and Do—Now* (Apr. 2, 2025), available here.

[45] Politico, *Former Washington Post employee launches class action suit against the outlet after massive data breach* (Dec. 5, 2025), available here.

[46] Red Hat, *Security update: Incident related to Red Hat Consulting GitLab instance* (Oct. 2, 2025), available here.

[47] Anthropic, *Disrupting the first reported AI-orchestrated cyber espionage campaign* (November 2025), available here; Paul, Weiss, *Anthropic Disrupts First Documented Case of Large-Scale AI-Orchestrated Cyberattack* (Nov. 25, 2025), available here.

[48] *Id.*

[49] Paul, Weiss, *Economic Sanctions and Anti-Money Laundering Developments: 2024 Year in Review* (Jan. 30, 2025), available here.

[50] U.S. Cybersecurity and Infrastructure Sec. Admin., Joint Cybersecurity Advisory, *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System* (Sept. 2025), available here.

Italian police arrested a Chinese national whom U.S. prosecutors identified as being part of another PRC state-sponsored threat actor group, Silk Typhoon.[51]

In March 2025, DOJ, the Naval Criminal Investigative Service and the Departments of State and Treasury announced a coordinated, whole-of-government response to illicit cyber activity by 12 PRC nationals, including two officers of the Ministry of Public Security.[52] The unsealed indictments charged computer intrusions, conspiracy and related offenses tied to multi-year campaigns targeting U.S. critical infrastructure and telecommunications networks, and described the use of front companies to procure infrastructure and obscure attribution. In parallel, the State Department announced related diplomatic measures, the Treasury Department designated associated entities and facilitators and CISA and the NSA issued a joint advisory detailing the actors' techniques, tactics and procedures and recommended mitigations.

One other area of focus for the federal government has been in combatting schemes by which individuals associated with the Democratic People's Republic of North Korea posed as IT workers in order to access networks of U.S. companies.[53] On November 14, DOJ announced five guilty pleas and more than $15 million in civil forfeiture actions against U.S. and foreign nationals in connection with such schemes.[54] According to DOJ's charging documents and pleading materials, for example, various U.S. persons assisted in providing IT workers to U.S. companies knowing that their identities were false, provided false identities to IT workers for use at U.S. companies and hosted hardware at their residences.[55]

Law enforcement also continued its efforts to hold accountable the threat actors responsible for a series of international ransomware attacks that plagued businesses across the globe in 2021. On May 1, DOJ announced the extradition of a Ukrainian national charged for his role in a series of international attacks using the Nefilim ransomware that targeted U.S., Canadian and Australian companies.[56] On December 19, 2025, DOJ announced that the defendant had pleaded guilty and faces 10 years in prison.[57]

Enforcement

Cybersecurity and the False Claims Act

The Department of Justice made cybersecurity a frontline False Claims Act ("FCA") priority in 2025, using the FCA to police representations made by government contractors about compliance with FAR/DFARS and NIST SP 800-171 requirements, even absent a breach. DOJ repeatedly emphasized that cybersecurity obligations are mission-critical contract terms, and that it thus intends to use the FCA to enforce misrepresentations.

A string of settlements—spanning defense, health, IT services, and life sciences—underscored that DOJ may treat misstatements about system security plans, controls scoring, patch and vulnerability management, usage of the Federal Risk and Authorization Management Program ("FedRAMP") and product security practices as material false claims, yielding significant penalties and multi-million-dollar relator shares.

You Should Know

DOJ's civil FCA settlements reflected broader trends in the regulation of government contractors:

- **National security concerns focused FCA scrutiny on cybersecurity compliance by defense and defense-adjacent contractors.** The majority of DOJ's cybersecurity FCA actions were focused on violations of cybersecurity provisions in

[51] The Record, *Chinese National Arrested in Milan after US Issues Arrest Warrant for Hafnium Attacks* (July 8, 2025), available here; Microsoft, *Silk Typhoon Targeting IT Supply Chain* (Mar. 5, 2025), available here.

[52] U.S. Dep't of Justice, *Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns* (Mar. 5, 2025), available here.

[53] U.S. Fed. Bureau of Investigation, *North Korean IT Worker Threats to U.S. Businesses* (July 23, 2025), available here.

[54] U.S. Dep't of Justice, *Justice Department Announces Nationwide Actions to Combat Illicit North Korean Government Revenue Generation* (Nov. 14, 2025), available here.

[55] *Id.*

[56] U.S. Dep't of Justice, *Ukrainian National Extradited from Spain to Face Conspiracy to Use Ransomware Charge* (May 1, 2025), available here.

[57] U.S. Dep't of Justice, *Ukrainian National Pleads Guilty to Conspiracy to Use Nefilim Ransomware to Attack Companies in the United States and Other Countries* (Dec. 19, 2025), available here.

defense contracts.[58] National security concerns appear to be driving DOJ to focus on defense contractor cybersecurity compliance, and any contractors in national security-adjacent businesses must be on high alert.

- **Cybersecurity compliance has moved to the top of DOJ's FCA agenda.** DOJ framed deficiencies in NIST, DFARS, and FAR requirements as actionable false claims, even where no breach or exploitation was alleged. Companies marketing software, equipment or services with embedded technology to government customers should assume their representations regarding cybersecurity are material to payment decisions and therefore FCA-relevant.

- **Robust documentation and candor proved decisive.** The FCA actions revealed the importance of proactive measures to both document security systems and remediate deficiencies in cyber defenses. Gaps in system security plans or inflated NIST scores drove liability, while prompt self-disclosure, cooperation and remediation materially mitigated penalties.

- **Robust documentation—and candor—are critical.** Recent FCA resolutions centered on the absence of an adequate system security plan,[59] as well as alleged misrepresentations of adherence to ISO and NIST standards.[60] Indeed the consequences of a false statement can be severe, as demonstrated by DOJ's criminal fraud prosecution of an employee of a government contractor for falsely certifying that his company's cloud platform complied with security controls under FedRAMP and the Department of Defense's Risk Management Framework, and for his efforts to obstruct an audit of those controls.[61] Companies should thus make sure they maintain contemporaneous documentation of security architecture, testing and monitoring, and should further take care that they exercise oversight of any marketing materials, proposals and certifications to ensure they accurately reflect the current state of controls.

- **Private-equity sponsors and acquiring entities can be at risk.** As demonstrated by DOJ's settlement with a defense contractor and its private equity sponsor owners for allegedly failing to implement NIST cybersecurity controls, owners and acquirers can face direct exposure for portfolio company conduct.[62] Sponsors should integrate rigorous cyber diligence and post-close compliance monitoring into their investment lifecycle. Additionally, strong acquisition due diligence must be implemented with a focus on cybersecurity measures taken by the target.

FTC and SEC Action

FTC Enforcement Actions

In 2025, the FTC continued to bring Section 5 actions against organizations that misrepresent their privacy or security practices, violate consumers' privacy rights or fail to maintain reasonable security for sensitive information, as well as for violations of the Children's Online Privacy Protection Act ("COPPA").

You Should Know

- **FTC enforcement priorities.** The actions underscore the FTC's priority on child protection online, emphasizing accurate age designations, robust parental consent and clear, non-deceptive monetization practices.

- **COPPA Rule amendments.** These actions also followed April 22, 2025, amendments to the COPPA Rule imposing additional restrictions on website and online service operators that collect personal information from children under the age of 13 and would, among other things:

[58] *See* U.S. Dep't of Justice, *Illinois Precision Machining Company Agrees to Pay $421,234 to Resolve Alleged False Claims Act Violations* (Dec. 5, 2025), available here; U.S. Dep't of Justice, *California Defense Contractor and Private Equity Firm Agree to Pay $1.75M to Resolve False Claims Act Liability Relating to Voluntary Self-Disclosure of Cybersecurity Violations* (Jul. 31, 2025), available here; U.S. Dep't of Justice, *Raytheon Companies and Nightwing Group to Pay $8.4M to Resolve False Claims Act Allegations Relating to Non-Compliance with Cybersecurity Requirements in Federal Contracts* (May 1, 2025), available here; U.S. Dep't of Justice, *Health Net Federal Services LLC and Centene Corporation Agree to Pay Over $11 Million to Resolve False Claims Act Liability Related to Cybersecurity* (Feb. 18, 2025), available here; U.S. Dep't of Justice, *Defense Contractor MORSECORP Inc. Agrees to Pay $4.6 Million to Settle Cybersecurity Fraud Allegations* (Mar. 26, 2025), available here.

[59] U.S. Dep't of Justice, *Raytheon Companies and Nightwing Group to Pay $8.4M to Resolve False Claims Act Allegations Relating to Non-Compliance with Cybersecurity Requirements in Federal Contracts* (May 1, 2025), available here.

[60] U.S. Dep't of Justice, *Illumina Inc. to Pay $9.8M to Resolve False Claims Act Allegations Arising from Cybersecurity Vulnerabilities in Genomic Sequencing Systems* (Jul. 31, 2025), available here.

[61] U.S. Dep't of Justice, *Senior Manager for Government Contractor Charged in Cybersecurity Fraud Scheme* (Dec. 10, 2025), available here.

[62] U.S. Dep't of Justice, *California Defense Contractor and Private Equity Firm Agree to Pay $1.75M to Resolve False Claims Act Liability Relating to Voluntary Self-Disclosure of Cybersecurity Violations* (Jul. 31, 2025), available here.

- expand the scope of protected personal information to include biometric identifiers;
- require operators to obtain separate verifiable parental consent before disclosing personal information collected from children for purposes that are not "integral" to operators' websites or online services; and
- mandate that operators establish, implement, and maintain a written information security program and data retention policy.[63]

In the first half of the year, FTC enforcement reflected a continuation of its historical emphasis on promoting consumer privacy rights. For instance, on January 14, 2025, the FTC finalized an order against Mobilewalla Inc.—a data broker that allegedly tracked and sold sensitive location data without adequate consent—banned its sales of certain location data and restricted its collection and use from sensitive places.[64] In addition, on May 21, 2025, the FTC finalized an order with GoDaddy—a major webhosting provider—over alleged data security lapses and misleading security representations, requiring a comprehensive information security program and independent assessments.[65]

September saw a cluster of actions centered on children's privacy and safety. On September 2, 2025, Disney agreed to pay a civil penalty and adopt additional controls after allegedly mislabeling child-directed videos on YouTube, enabling collection and use of children's personal data for advertising in violation of COPPA.[66] On September 3, 2025, the FTC announced a settlement with Apitor Technology over alleged violations of COPPA tied to collection of children's geolocation data through an app without verifiable parental consent.[67] And on September 29, 2025, the FTC sued Iconic Hearts Holdings, Inc. (Sendit) and its CEO for allegedly collecting children's personal information without parental consent and deceiving users about paid features—combining COPPA, Section 5 deception and negative-option concerns.[68]

SEC Dismisses Cybersecurity Lawsuit Against SolarWinds

The SEC announced on November 20, 2025, that it had jointly stipulated with SolarWinds Corporation and its CISO to dismiss the agency's cyber-disclosure enforcement action. The SEC emphasized that this decision "does not necessarily reflect" its position on other cases. The litigation, filed in 2023 and amended in 2024, had alleged misleading cybersecurity statements and disclosures stemming from the December 2020 SUNBURST supply chain attack. The SEC's announcement followed a court ruling that left only limited misrepresentation and scheme claims in play while rejecting most other theories, including challenges to the company's December 2020 Form 8-K disclosures and internal accounting controls claims.

SEC Cyber and Emerging Technologies Unit

On February 20, 2025, the SEC announced the creation of a new Cyber and Emerging Technologies Unit ("CETU") to target cyber-related misconduct and protect retail investors from bad actors in the emerging technology space.[69] The new unit, which replaces the Crypto Assets and Cyber Unit, will include about 30 fraud specialists and attorneys across multiple SEC offices.

You Should Know

The SEC has identified seven priority areas that the CETU will focus on, including:

- fraud committed using emerging technologies, such as AI and machine learning;
- use of social media, the dark web or false websites to perpetrate fraud;
- hacking to obtain material nonpublic information;
- takeovers of retail brokerage accounts;

[63] *See* 16 CFR Part 312. While the amended Rule became effective on June 23, 2025, regulated entities generally have until April 22, 2026 to comply.

[64] FTC, *FTC Finalizes Order Banning Mobilewalla from Selling Sensitive Location Data* (Jan. 14, 2025), available here.

[65] FTC, *FTC Finalizes Order with GoDaddy over Data Security Failures* (May 21, 2025), available here.

[66] FTC, *Disney to Pay $10 Million to Settle FTC Allegations the Company Enabled the Unlawful Collection of Children's Personal Data* (Sept. 2, 2025), available here.

[67] FTC, *FTC Takes Action Against Robot Toy Maker for Allowing Collection of Children's Data without Parental Consent* (Sept. 3, 2025), available here.

[68] FTC, *FTC Alleges Sendit App and its CEO Unlawfully Collected Personal Data from Children, Deceived Users About Messages, Subscription Memberships* (Sept. 29, 2025), available here.

[69] SEC, *SEC Announces Cyber and Emerging Technologies Unit to Protect Retail Investors* (Feb. 20, 2025), available here.

- fraud involving blockchain technology and crypto assets;
- regulated entities' compliance with cybersecurity rules and regulations; and
- public issuer fraudulent disclosure relating to cybersecurity.

The reconfigured unit comes as part of an SEC shift away from targeting established companies within the financial industry to focusing instead on broader cybercrimes or issues that impact retail investors across industries. In particular, it appears to signal a shift in the SEC's focus around cryptocurrency that emphasizes more structured rulemaking over enforcement actions.[70]

State Enforcement

This year has seen a marked escalation in state-level privacy and cybersecurity enforcement, particularly with respect to cooperation among states. For example, California, Colorado, Connecticut, Delaware, Indiana, New Jersey, Oregon, Minnesota and New Hampshire formed the Consortium of Privacy Regulators to coordinate resources and privacy enforcement;[71] and the attorneys general of California, Colorado, and Connecticut announced a joint investigative sweep of potential noncompliance with the Global Privacy Control and consumer opt-out requirements.[72]

You Should Know

- **Escalating state enforcement and mega-penalties.** States are imposing record-breaking fines and settlements across privacy and cybersecurity, including Texas's $1.375 billion action against Google and California's seven-figure penalties against major brands, signaling aggressive scrutiny of biometric/geolocation tracking, disclosures and data sharing.
- **Operational compliance focus.** State regulatory actions focused on failures in consumer opt-out mechanisms, excessive verification burdens, inadequate privacy notices for applicants and consumers, missing processor contracts and protections for children—reinforcing expectations for clear notices, effective opt-outs and vendor governance.
- **Enforcement actions beyond Texas, California and New York.** While these state regulators remained the most significant jurisdictions for regulatory action under state privacy and cyber regimes, other states, including Connecticut, Florida and Oregon, are ramping up first-of-their-kind actions.

Individual state enforcement of privacy and cybersecurity violations has also continued, with states focusing on privacy opt-out mechanisms and notices, children's privacy rights, timely incident reporting, biometric data and national security concerns, and verifiable vendor governance.

Texas

In May 2025, the Texas Attorney General announced one of the largest ever recorded state-enforced privacy penalties, totaling $1.375 billion against Google for its alleged unlawful tracking and collection of personal biometric information and geolocation data.[73]

Texas has also increased its enforcement of privacy laws in relation to national security through the Texas Data Privacy and Security Act. For instance, the Texas Attorney General announced in May that it had sent noncompliance notices to several Chinese companies, including Alibaba and Capcut, for failing to disclose whether they process consumer data, allow consumers to opt out of data collection and enable consumers to delete their personal data.[74]

[70] *See also* SEC, SEC Crypto 2.0: Acting Chairman Uyeda Announces Formation of New Crypto Task Force (Jan. 21, 2025), available here.

[71] California Privacy Protection Agency, *State Regulators Form Bipartisan Consortium to Collaborate on Privacy Issues* (Apr. 16, 2025), available here.

[72] California Privacy Protection Agency, *California Privacy Protection Agency Announces Joint Investigative Privacy Sweep: CA, CO, and CT Investigate Businesses Refusing to Honor Consumers' Right to Opt-Out of the Sale of Their Personal Information* (Sept. 9, 2025), available here.

[73] Texas Attorney General, *Attorney General Ken Paxton Secures Historic $1.375 Billion Settlement with Google Related to Texans' Data Privacy Rights* (May 9, 2025), available here.

[74] Texas Attorney General, *Attorney General Ken Paxton Takes Legal Action Against Chinese Companies Violating Texans' Privacy Rights* (May 6, 2025), available here.

California

California continues to be the most active state in privacy and cybersecurity enforcement. Prominent enforcement actions by California regulators included a March 2025 fine issued by CalPrivacy against Honda Motor Co. for allegedly insufficient opt-out mechanisms. CalPrivacy alleged that before allowing Californians to opt out of the sale or sharing of personal information, Honda required that Californians verify themselves and provide excessive personal information.[75]

Furthermore, in September 2025, CalPrivacy issued a $1.35 million fine against Tractor Supply Company, the nation's largest rural lifestyle retailer, for the alleged failure to notify California job applications of their privacy rights, provide consumers with effective opt-out mechanisms and maintain sufficient privacy policies; as well as for disclosing personal information to third parties without entering into proper data privacy agreements.[76] And the following month, the California Attorney General secured a $530,000 settlement with Sling TV for its alleged failure to provide consumers with an easy-to-use method for preventing the sale of their personal information, and for failing to provide sufficient privacy protections for children.[77]

New York

As described in part above, NYDFS has continued its rigorous enforcement of Part 500 and related cybersecurity regulations, underscoring its expectation that covered entities strictly comply with timely incident reporting, robust incident response planning, updated data inventories and senior-level annual certifications. NYDFS started the enforcement year off quickly, announcing a $2 million settlement with PayPal in January for allegedly failing to use qualified personnel to manage key cybersecurity functions, and for failing to provide adequate training to address cybersecurity risks.[78]

In October, NYDFS announced a $19 million penalty against eight automobile insurers, alleging that their inadequate cybersecurity controls allowed hackers to steal New Yorkers' personal information, including driver's license numbers and dates of birth from online automobile insurance quoting applications.[79] Beyond the underlying breaches, NYDFS emphasized that delayed reporting can convert a security lapse into a compliance failure under Part 500, with the 72-hour notification clock running from the covered entity's determination that a reportable cybersecurity incident has occurred.

And in August, NYDFS reached a $2 million consent order with Healthplex, an insurance agent, following a phishing-driven email compromise.[80] DFS alleged multiple control failures, including a lapse in MFA, an absence of workable data retention and proper disposal processes, an almost five-month delay in notifying DFS and improper annual certifications. The NYDFS order included remediation requirements that the insurance agent retain a third-party auditor to assess MFA controls, among other things.

Other States

Texas and California have not been alone in escalating privacy-related enforcement activity. In the first monetary penalty under Connecticut's consumer privacy statute, Connecticut obtained an $85,000 settlement against TicketNetwork, an online ticket marketplace, for its alleged failure to comply with the Connecticut Attorney General's cure notice regarding its deficient privacy notice.[81] The Connecticut Attorney General also announced that it has issued at least four separate privacy notice sweeps this year, consisting of over two dozen cure notices aimed at addressing privacy notice deficiencies.

In October 2025, the Florida Attorney General announced its first-ever Florida Digital Bill of Rights suit against Roku, alleging that Roku willfully collected and sold children's personal data without parental notice or consent.[82] And while Oregon's universal opt-out requirements do not begin until 2026, the Oregon Attorney General announced in August 2025 that it has

[75] California Privacy Protection Agency, *Honda Settles With CPPA Over Privacy Violations* (Mar. 12, 2025), available here.

[76] California Privacy Protection Agency, *Nation's Largest Rural Lifestyle Retailer to Pay $1.35M Over CCPA Violations* (Sept. 30, 2025), available here.

[77] California Privacy Protection Agency, *Attorney General Bonta Secures $530,000 Settlement with Sling TV, First Enforcement Action from DOJ's Sweep of Streaming Services* (Oct. 30, 2025), available here.

[78] New York Dept. of Fin. Servs., *Superintendent Adrienne A. Harris Secures $2 Million Cybersecurity Settlement with PayPal, Inc.* (Jan. 23, 2025), available here.

[79] New York Dept. of Fin. Servs., *Superintendent Harris Secures More than $19 Million from Auto Insurance Companies over Data Breaches* (Oct. 14, 2025), available here.

[80] New York Dept. of Fin. Servs., *Superintendent Adrienne A. Harris Secures $2 Million Cybersecurity Settlement with Healthplex, Inc.* (Aug. 14, 2025), available here.

[81] Connecticut Attorney General, *Attorney General Tong Announces $85,000 Settlement with TicketNetwork for Violations of the Connecticut Data Privacy Act* (July 8, 2025), available here.

[82] Compl., *Office of Attorney General, State of Florida* v. *Roku, Inc.*, Doc. No. 233525993 (Oct. 13, 2025), available here.

investigated 91 consumer complaints for violations of Oregon's Consumer Privacy Act ("OCPA") in the last two years, including initiating and closing 38 cure letters for OCPA-related violations.[83]

Privacy and Cyber Litigation

Plaintiffs Face Challenges to Standing in Data Breach Litigation

This year, federal courts have raised the bar for plaintiffs to establish standing in data breach cases, sending a clear message that "[h]aving personal information exposed in a data breach—which has happened to everyone—is not enough to sue."[84] After the Supreme Court's 2021 decision in *TransUnion* v. *Ramirez*, courts are increasingly requiring plaintiffs to allege actual misuse of personal information to meet the injury-in-fact element of Article III standing.

Many courts have now adopted the test from *McMorris* v. *Carlos Lopez & Associates LLC* (2d Cir. 2021) to determine whether a future harm is "actual or imminent."[85] Among the factors in the *McMorris* test is whether there has been actual misuse of any data exposed from the alleged breach.[86] While some courts within the Second Circuit have held that not all of the *McMorris* factors need not be met for standing to be established,[87] the majority of district courts to consider the issue post-*TransUnion*, including the District of Utah in *In re Progressive Data Breach Litigation*, have required plaintiffs to allege actual misuse.[88] Trial courts in 2025 have begun to move away from precedent that found standing for plaintiffs based solely on the occurrence of a data breach, and instead require allegations of "actual misuse of data" under the *McMorris* test.[89]

Plaintiffs Face Enhanced Pleading Standards for California Invasion of Privacy Act Claims

The California Invasion of Privacy Act ("CIPA") makes it unlawful to intercept the contents of a communication without the consent of all parties to the communication. Plaintiffs have used CIPA to challenge the use of pixels, cookies and other web-based trackers, on the grounds that the use of such third-party technologies, which capture user activity on websites, amount to an illegal wiretap under CIPA. Over the past year, courts tightened the pleading standards under CIPA for web-tracking cases and clarified where claims can still survive.

You Should Know

- **Categories of CIPA Claims.** Section 631 of CIPA prohibits the interception of communications or the actual or attempted review of communication contents without consent. Section 632 of CIPA prohibits the intentional recording or eavesdropping on a "confidential communication" without the consent of all parties involved. Section 638.51 prohibits installing or using a "pen register" or "trap and trace" devices designed to track routing information such as IP addresses, without a court order.

- **Actual interception of communication content by a non-party is required to make out a Section 631 claim.** Complaints survive only when they plead program-specific, real-time interception of the "contents" of

[83] Oregon Dep't of Justice, *Enforcement Report: The Oregon Consumer Privacy Act, The First Year* (Aug. 2025), available here.

[84] The Wall Street Journal, *'No Harm, No Foul:' Courts Take Tougher Line on Data-Breach Suits* (Sept. 26, 2025), available here.

[85] "[C]ourts have been more likely to conclude that plaintiffs have established a substantial risk of future injury where they can show that at least some part of the compromised dataset has been misused – even if plaintiffs' *particular* data subject to the same disclosure incident has not yet been affected." *McMorris* v. *Carlos Lopez & Associates LLC*, 995 F.3d 295, 301 (2d Cir. 2021).

[86] *See Murray* v. *Connecticut College*, 2025 WL 2712664, at *5 (D. Conn. Sep. 23, 2025) (quoting *McMorris*, 995 F.3d at 301) (holding "[t]he second *McMorris* factor asks whether the plaintiff can show that at least some part of the compromised dataset has been misused") (quotations omitted).

[87] "Because Murray satisfies two of the three *McMorris* factors, I find that he has plausibly alleged an imminent injury. This result accords with the result in *Bohnak*, where the Court also found that the plaintiff satisfied two of the three factors and therefore 'sufficiently alleged that she faces an imminent risk of injury.' *Id*. at *6 (quoting *Bohnak* v. *Marsh & McLennan Cos., Inc.*, 79 F.4th 276, 288 (2d Cir. 2023)).

[88] "The Second Circuit held that mere increased risk of identity theft can be a concrete injury, although courts are more likely to so conclude when plaintiffs can show that at least some part of the compromised dataset has been misused – even if plaintiffs' particular data subject to the same disclosure incident has not yet been affected." *In re Progressive Data Breach Litig.*, 2025 WL 213744, at *5 (D. Utah Jan. 16, 2025).

[89] For example, this trend was articulated in *In re Lurie Children's Hospital Data Sec. Litig.*, by Judge Andrea Wood, "[a]s a result of TransUnion, Plaintiffs are squarely foreclosed from predicating their standing solely on the imminent risk of identity theft that they claim to face from the unauthorized disclosure of their PII and PHI in the Data Breach." 2025 WL 2754760 *6, (N.D. Ill. Sep. 27, 2025) (holding the Seventh Circuit's opinion in *Remijas* v. *Nieman Marcus Grp., LLC*, 794 F.3d 688, 692 (7th Cir. 2015), that an increased risk of future fraud and identity theft as a result of a data breach can be sufficient to support Article III standing should not be followed in light of TransUnion). Other district courts in 2025 have predicted that their circuits will adopt this trend, "district courts throughout the Tenth Circuit have predicted that the Court of Appeals will require actual misuse of stolen data to find that plaintiffs have standing, and the court applies this standard here."*Stern* v. *Academy Mortgage Corp.*, 2025 WL 239036 *3 (D. Utah Jan. 17, 2025). *See also*, *Stuart* v. *Stuart Kyocera A VX Components Corp.*, 769 F.Supp.3d 476, 491 (D.S.C. 2025) (granting motion to dismiss for lack of standing under Fourth Circuit case law requiring plaintiffs to allege "actual misuse" of personal information).

communications—often with screenshots/demos—and plausibly allege a non-party vendor reads and repurposes those contents for its own use. Activity falling below that threshold, such as "tracking," post-hoc storage of communications or the collection of information other than communication contents (e.g. button clicks) are regularly found insufficient to support a claim under Section 631. A pair of Ninth Circuit decisions issued within days of one another in June 2025 helped to clarify the requirements for a viable CIPA claim. In *Thomas* v. *Papa John's*, the Court of Appeals affirmed the dismissal of a CIPA claim holding that a party cannot be liable for eavesdropping on its own conversation, and in *Mikulsky* v. *Bloomingdale's, LLC,* the Court reversed the dismissal of a CIPA claim in which the defendant allegedly used session-replay code to capture and disclose the contents of website communications to a third-party vendor without user consent.[90] Together, these cases make clear that vendor-interception theories—not direct eavesdropping by the website—drive viable CIPA claims.

- **Chat-feature claims under CIPA have largely stalled.** Courts in the Central and Southern Districts of California have repeatedly held that CIPA provisions prohibiting eavesdropping target calls between specified telephones, and not browser-based chats, even on smartphones. Plaintiffs are pivoting back to claims under Section 631, but many claims still fail absent plausible allegations that a third-party vendor read and used chat contents for its own purposes.

Litigation Under Biometric Privacy Laws Continued to Increase

Biometric litigation was active in 2025, continuing a trend seen in 2024. While court decisions and statutory amendments in 2024 sought to limit both the scope and damages awards from actions under Illinois' Biometric Information Privacy Act ("BIPA"), BIPA litigation has remained robust in 2025. Other states—most notably Washington—also entered the arena with biometric laws that provided private rights of action.

Enforcement activity under state biometric laws has also been significant. For example, as described above, the Texas Attorney General reached a settlement with Google for $1.375 billion, resolving allegations that Google unlawfully tracked and collected users' private data regarding geolocation, incognito searches and biometric data.[91]

You Should Know

- **Illinois' BIPA remains the designated law of choice despite 2024 reforms.** Despite BIPA reforms narrowing its applicability and usage, BIPA class actions continued apace in 2025, with large settlements across sectors. However, a certified appeal regarding the retroactivity of BIPA amendments could change this trend in 2026.

- **Enforcement and private litigation is expanding beyond Illinois.** Texas secured a record $1.375 billion settlement over alleged unlawful biometric and geolocation tracking, and litigation in Washington under its newly enacted My Health My Data Act ("MHMDA") will likely increase. Several states are also considering enacting biometric-specific statutes, signaling potential new forums for plaintiffs.

- **Risk now reaches "biometric-adjacent" data and ad-tech stacks.** Plaintiffs and the government are now targeting software development kits ("SDKs"), analytics and advertising tools that may infer health-related activity or capture identifiers tied to biometric processing. Companies should consider mapping any biometric capture or use, verify notice/consent and retention practices and flow-down obligations to vendors operating within web, mobile and cloud environments.

In Illinois, some commentators suspected that BIPA litigation would slow in 2025 following multiple court decisions narrowing the applicability of BIPA,[92] as well as 2024 statutory amendments limiting the scope of BIPA's damages by replacing a "per-scan" accrual theory with a single recovery per person for repeated collection or disclosure via the same method.[93] But that slow-down failed to materialize. For example, in March 2025, Clearview AI agreed to pay $51.75 million to a nationwide class alleging that its automatic collection, storage and use of biometric data violated BIPA.[94] Motorola Solutions settled a class action for $47.5 million in June related to allegations that it collected, stored and used residents' biometric data in connection

[90] *Thomas* v. *Papa John's Int'l, Inc.*, 2025 WL 1704437, at *1 (9th Cir. June 18, 2025); *Mikulsky* v. *Bloomingdale's, LLC*, 2025 WL 1718225, at *1 (9th Cir. June 20, 2025).

[91] Texas Attorney General, *Attorney General Ken Paxton Secures Historic $1.375 Billion Settlement with Google Related to Texans' Data Privacy Rights* (May 9, 2025), available here.

[92] Security Industry Assoc., *Key Dismissal of BIPA Case Upheld in Federal Court: What SIA Members Need to Know* (July 3, 2024), available here.

[93] American Bar Association, *How Will the Recent Amendments to Illinois's BIPA Affect the Use of Biometric Data?* (Sept. 4, 2024), available here.

[94] Nat'l L. Rev, *A First in BIPA Litigation: Class Members Receive Equity in Clearview AI* (July 22, 2025), available here.

with providing law enforcement with its facial recognition technology and access to booking photos.[95] In August, Speedway settled a class action for $12 million in connection with allegations that its use of finger scanners to track employee hours without proper notice and consent procedures violated BIPA.[96] That same month, Google settled claims by students for $8.75-million alleging that it was collecting their biometric data through its Workspace for Education platform.[97]

Beyond BIPA, other states have expanded their biometric data regulations. In February 2025, the first lawsuit invoking Washington state's MHMDA was filed, testing a sweeping private right of action around consumer health data that explicitly encompasses biometric and sensitive location data.[98] The case challenges the use of advertising SDKs to collect biometric and location information allegedly indicative of health-related activity, positioning Washington as a potential new forum for biometric-adjacent claims that operate outside traditional comprehensive privacy statutes.

Meanwhile, lawmakers in several states have advanced biometric-specific bills, including consideration of a New York Biometric Privacy Act,[99] and pending proposals for similar laws in Massachusetts[100] and Missouri.[101] This activity, combined with aggressive state attorneys general in leading jurisdictions and a maturing plaintiffs' bar, points to a broader geographic distribution of biometric litigation risk, even if Illinois and Texas still remain focal points.

Telemarketing: Updates to the TCPA

The TCPA litigation landscape in 2025 was shaped by fast-moving court and agency action around consent and revocation.

You Should Know

- **The end of the One-to-One consent rule.** In January 2025, the Eleventh Circuit struck down the FCC's "One-to-One consent" rule.[102] That rule required a person's permission to be given to only one seller at a time to prevent "lead generators" from selling a single consent to many sellers. Overturning the rule disrupted the FTC's plan to require consent that is both seller-specific and limited to a specific subject, and it immediately created uncertainty for companies preparing for the January 27, 2025, effective date of the rule.

- **New consent requirements under the Opt-Out Rule.** The FCC's "Opt-Out Rule" took effect on April 11, 2025. The Opt-Out rule tightens requirements for how consumers can revoke consent by requiring businesses to accept opt-outs through any reasonable method, to process them within 10 business days and—if someone opts out after an informational message—to stop both informational and marketing robocalls and robotexts. After receiving comments from industry, the FCC granted a limited waiver delaying the toughest requirement—treating an opt-out to one type of message (like promotional) as applying to all future robocalls and robotexts—until April 11, 2026. The other obligations still apply in 2025.

- **Potential updates to the TCPA.** As of fall 2025, the FCC was considering broader TCPA changes that could significantly affect future lawsuits if adopted. A draft proposal (FNPRM) suggested eliminating older rules like the "call abandonment" safe harbor and some company-specific do-not-call list obligations. It also asked whether businesses could require consumers to use specific channels to revoke consent instead of accepting revocations by "any reasonable means."

- **Higher litigation risk.** Together with the Supreme Court's 2024 holding that trial courts need not defer to agency interpretations in civil cases, these developments signaled more inconsistency from court to court and encouraged challenges to long-standing TCPA rules.

---

[95] Chloe Gocher, *$47.5M Motorola Solutions Settlement Resolves Class Action Lawsuit Over Alleged FaceSearch BIPA Violations* (June 3, 2025), ClassAction.org, available here.

[96] Chloe Gocher, *$12M+ Speedway Settlement Ends Class Action Lawsuit Over Alleged Biometric Privacy Violations* (Sept. 11, 2025), ClassAction.org, available here.

[97] Kelsey McCroskey, *$8.75M Google Settlement Resolves Class Action Lawsuit Over Alleged Chromebook Privacy Violations* (Aug. 1, 2025), ClassAction.org, available here.

[98] Meredith Garrity, *My Health My Data Act: A New Class Action Suit Puts Washington's Health Data Privacy Law in the Spotlight* (May 6, 2025), Suffolk U. Law School, available here.

[99] New York Senate Bill S1422 (last accessed Dec. 21, 2025), available here.

[100] Massachusetts Legislature, *Fact Sheet & Highlights: The Massachusetts Data Privacy Act S.2608* (Sept. 18, 2025), available here.

[101] Missouri Senate Bill 554 (Aug. 28, 2025), available here.

[102] *Insurance Marketing Coalition* v. *FCC*, No. 24-10277 (11th Cir. Jan. 24, 2025).

* * *

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

Katherine B. Forrest
+1-212-373-3195
kforrest@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

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

Ian C. Richardson
+1-202-223-7405
irichardson@paulweiss.com

Jacobus "Janus" Schutte
+1-212-373-3152
jschutte@paulweiss.com

Jennifer Songer
+1-202-223-7467
jsonger@paulweiss.com

Audrey M. Paquet
+1-212-373-2397
apaquet@paulweiss.com

Associates Sophie Bergman, Walter Bonné, Neil Chitrao, Noah Cohen, Matthew J. Disler, Rachel Gallagher, Corey J. Goldstein, Cenadra Gopala-Foster, Patrick Lim, Cole A. Rabinowitz, Samuel Rebo and Amanda Valerio-Esene, and law clerk Maggie E. Riley contributed to this Client Memorandum.