Now & Next
Privacy and Technology Alert

February 9, 2026

Data Privacy, Cybersecurity, AI developments shaping 2026

By Jacqueline Cooney, Jenny Holmes, and Hannah Edmonds

Key changes in data privacy, cybersecurity, and AI throughout 2025 are already shaping the outlook for 2026 and beyond.

What's the impact?

- Regulatory focus is intensifying on data security and AI risk, with DOJ cross-border data rules and NIST's draft AI guidance elevating national-security and enterprise-level responsibilities.
- A growing gap between evolving state privacy and AI mandates and a lighter federal approach is creating legal uncertainty and escalating compliance complexity.
- Expanded COPPA interpretations, heightened FTC enforcement, and delayed but looming rules like CIRCIA are pushing organizations to reassess sensitive-data practices and strengthen incident-response and reporting capabilities.

Over the course of 2025, we have seen several key developments in the fields of data privacy, cybersecurity, and artificial intelligence (AI). Below are a few developments highlighted along with what they mean for 2026 and beyond.

DOJ "bulk data transfer" rule implemented

The Department of Justice (DOJ) implemented a new regime—the "Data Security Program"—which creates the bulk data transfer rule (the Rule), which restricts transfers of bulk US sensitive personal data and government-related data to "countries of concern." Unlike typical privacy regulations that focus on consumer protection, the Rule serves to protect US national security. "Countries of concern" include China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela. The Rule comes with significant civil and criminal penalties for noncompliance.

The Rule took effect on April 8, 2025, with full compliance enforceable as of October 6, 2025. This development raises immediate cross-border diligence and contract needs for vendor, employment, investment, and data brokerage arrangements. Affected organizations can expect continued increase in compliance burdens since the Rule requires self-evaluations and operations audits for transparency into where bulk US data is transferred and by whom that data is accessed outside of the US. This increased burden means that organizations must allot additional time and resources toward compliance efforts.

NIST AI and cybersecurity integration draft guidance

In December 2025, the National Institute of Standards and Technology (NIST) released a preliminary draft of the Cybersecurity Framework (CSF) Profile for AI (the Guidance). The Guidance is intended to assist organizations with managing cybersecurity risks uniquely associated with AI systems while also leveraging AI to improve organizations' security posture. The draft Guidance received public comment until January 30, 2026, with the final version expected to further evolve in 2026.

In following the Guidance, organizational cybersecurity risk management processes should generally expand to cover AI-specific vulnerabilities. Organizations that already use the NIST Cybersecurity Framework can map AI-specific considerations into existing security controls. Demonstrating adherence to the Guidance could serve as a key market differentiator that will allow organizations to foster greater trust with clients and the public.

State AI regulation emerges; White House responds

Colorado enacted the first comprehensive state AI law, the Colorado Artificial Intelligence Act (CAIA), effective as of May 17, 2024, to govern "high-risk" AI systems. The CAIA requires risk management for AI-driven decisions in employment, housing, and healthcare and will be implemented as of June 30, 2026 (delayed from February 1, 2026). California also passed multiple AI transparency and sectoral laws—driving impact assessment, discrimination-mitigation, and transparency controls for developers and deployers. The California laws are scheduled to take effect in 2026. In response, the White House's July 2025 AI Action Plan and a December 2025

executive order promote a minimally burdensome national framework and discourages state-level AI mandates. This contrast to the emergence of state AI regulation creates legal uncertainty, but it does not displace existing state privacy and AI laws, absent further rulemaking or litigation.

Organizations will continue to face a challenge to both comply with state AI law obligations and to account for the White House's minimally burdensome approach to AI regulation. This challenge impacts innovation and legal risk management since it requires organizations to develop flexible AI governance that prepares them for conflicts between state mandates and potential federal preemption efforts.

FTC sharpens COPPA and sensitive-data enforcement

On January 16, 2025, the Federal Trade Commission (FTC) finalized changes to the Children's Online Privacy Protection Act (COPPA) Rule, adopting certain amendments proposed in early 2024. Those amendments include changes to notice requirements, additional methods for verifiable consent, expansion of the definition of "personal information," updated data retention requirements, and updated Safe Harbor program requirements. Notably, the FTC recently brought actions against data brokers and platforms over sensitive location and children's data, which underscores broader definitions of "sensitive" data and demanding updates to consent, minimization, retention limits, and security programs. For example, in September 2025, the FTC sued a messaging app for collecting minors' personal information without required COPPA parental consent. This suit is currently active and pending.

The expansion of the definition of "personal information" under COPPA to include biometrics along with stricter data retention requirements and the requirement of separate parental consent for disclosing children's data to advertisers is prompting organizations to reevaluate to what extent they may be in scope with COPPA. This may require that those organizations update their processes to incorporate COPPA compliance initiatives. Further, organizations handling sensitive data, such as precise geolocation data, children's data, and biometric data, generally have heightened compliance obligations and are therefore more susceptible to FTC enforcement.

CIRCIA incident-reporting timeline delayed

The Cybersecurity and Infrastructure Security Agency (CISA) delayed its final rule for the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) until May 2026. This pushes back the requirement for entities to report cyber incidents within 72 hours and ransomware payments within 24 hours. The extension is intended to ease industry burden by providing more time for industry stakeholders to prepare for compliance. The delay leaves sectoral and state rules to continue to govern the reporting of incidents.

As the final rule's effective date approaches, entities that are part of the critical infrastructure sectors, as defined by CISA, should proactively update incident response plans to account for CIRCIA notification procedures and deadlines. Entities should also proactively establish ransomware payment protocols and assess the cybersecurity practices of their third-party vendors.

State privacy law map expanded; existing laws see additional changes

By the end of 2025, 19 US states enforced comprehensive privacy laws, with several new statutes effective in 2026. This complicates the multi-state privacy compliance obligations for organizations across industries. Colorado and California added "neural data" (and Colorado also added "biological data") to "sensitive" data definitions. These additions to "sensitive" data definitions expand high-risk classifications and consent duties for neurotech and adjacent use cases. Oregon expanded protection for children's personal data as well as for all Oregon residents' precise geolocation data, including that the sale of precise geolocation data is banned. California, Colorado, and Connecticut also launched a joint investigative sweep to enforce compliance with Global Privacy Control.

As additional state privacy laws come into force and existing privacy laws continue to evolve, the patchwork of legal obligations that organizations face will continue to expand. Organizational compliance initiatives must be flexible to account for new state privacy compliance obligations.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Jacqueline W. Cooney
617.345.6180
jcooney@nixonpeabody.com

Jenny L. Holmes
585.263.1494
jholmes@nixonpeabody.com

Hannah Edmonds
202.585.8370
hedmonds@nixonpeabody.com