KPMG

Regulatory Alert

Regulatory Insights

March 2025

First 100 Days: Upcoming Regulatory Signals for Cyber and Privacy

KPMG Regulatory Insights

- **Innovating Cyber & Protecting Privacy:** Recognition of cyber risks, and the interplay between innovation and data privacy amidst priorities for innovation, speed and competitiveness.
- **Shifts in Federal Role:** Infrastructure and cyber preparedness a focus of states; a general pullback on federal advisory councils.
- **State Expansion:** State privacy and cyber bills expand in concert with proposed AI legislation; efforts to “fill the gap”.

Shifts in AI regulation have occurred at different The new Administration acted early to pull back prior advisory councils focused on cyber and privacy though direct actions to change the overall regulatory trajectory at the federal level appear limited. States, however, have continued to actively pursue cyber- and privacy-related legislation/regulation in these areas, often in relation to AI. Signals for potential regulatory change can be seen in:

1. Federal actions/directives, including a pullback on regulatory outreach/advisory committees, redirection of infrastructure responsibilities to the states, congressional activity, and the issuance of new regulatory rules, tools, and frameworks.
2. State laws and regulations, including an expanding number and variety of cyber and privacy expectations across many states, creating a patchwork of regulatory responsibilities.

1. Federal Actions/Directions

Actions and directives at the federal level may serve as indicators of ongoing efforts to reshape the regulatory environment for cyber and privacy. Regulatory signals include:

Signals	Description/Examples	Source
Pullback on Regulatory Outreach/ Advisory Committees	Dismantling of advisory boards, including terminating: • All members of the Cyber Safety Review Board (CSRB) and the AI Safety and Security Board • Select members of the Privacy and Civil Liberties Oversight Board (PCLOB) • The Critical Infrastructure Partnership Advisory Council (CIPAC), the Data Privacy and Integrity Advisory Council, and the Cyber Investigations Advisory Board Uncertainty regarding future of public/private partnership to review and assess cyber incidents Uncertainty regarding future functionality of the PCLOB to protect privacy and civil liberties by national securities agencies	DHS Notice
	Potential for reduced size and scope of varying agencies/functions, based on reductions in workforce	Multiple News Reports
Redirection of Responsibility to States	Implementation of Executive Order on “Achieving Efficiency Through State and Local Preparedness”, which directs State and local governments to play a more active role in infrastructure resilience and preparedness including prioritization and strategic investment “to address risks, including cyber attacks”. Also calls for a: • National Resiliency Strategy (due June 2025) • National Critical Infrastructure Policy (to be risk-based - due September 2025) • National Risk Register (due November 2025) Reconsideration of select National Security Memorandums and Executive Orders related to Critical Infrastructure Security and Resilience and Supply Chains	White House
Congressional Activity	Continuation of Congressional hearings considering harmonization of cyber regulations/reporting requirements, including reciprocal recognition across critical infrastructure sectors. Issues include: • Costs vs benefits of duplicative reporting • Reconsideration of CISA proposed rule to implement the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) • Reconsideration of SEC Cybersecurity Disclosure Rule • Coordination between government and private sector	U.S. House Committee on Homeland Security hearing

Congressional Activity (cont.)	Consideration of AI Cyber Defense (consistent with EO 14144)	Senate Armed Services Subcommittee hearing
Issuance of Regulations, Tools and Frameworks	Development of a new cloud-native approach to cybersecurity assessment and authorization programs (FedRAMP 20x) with the intent to speed-up timeframe for agencies to get access to the latest technology	GSA Announcement
	Consideration of draft guidance ("Quick Start Guide") for NIST Cybersecurity Framework 2.0: Cybersecurity, Enterprise Risk Management, and Workforce Management, which promotes alignment of cybersecurity risk management, ERM, and workforce management practices, including: • Adoption of established frameworks as industry standards • Promotion of continuous assessment and improvement protocols • Potential for workforce assessments and upskilling initiatives • Best practices to include detailed Organizational Profiles and risk management documentation	NIST Special Publication
	Retention of data privacy-related rules to protect against transactions involving foreign-connected hardware and/or software (and related supply chains) that collect data on U.S. consumers (e.g., Department of Commerce final rule on Connected Vehicles – effective March 2025) and may pose potential risks to consumers (e.g., sensitive consumer data such as biometric, geolocation data) or national security.	DOC Final Rule
	Expectation that the Department of Justice final rule on transactions involving Bulk Sensitive Personal Data will go into effect in April 2025	DOJ Final Rule
	Potential to revisit recent FTC amendments to the Children's Online Privacy Protection Rule ("COPPA") re: parental consent, indefinite data retention, age verification-related data collection	FTC Statement
	Formation of the Cyber and Emerging Technologies Unit to focus on cyber-related misconduct related to securities transactions, including fraud committed using emerging technologies, hacking to obtain nonpublic information, account takeovers, compliance with cybersecurity laws and regulations, and disclosures.	SEC Announcement

Note: Thus far, cybersecurity Executive Orders from the previous Administration (EO 14028 – Improving the Nation's Cybersecurity (May 2021), and EO 14144 – Strengthening and Promoting Innovation in the Nation's Cybersecurity (January 2025)) remain in place.

1. State Laws

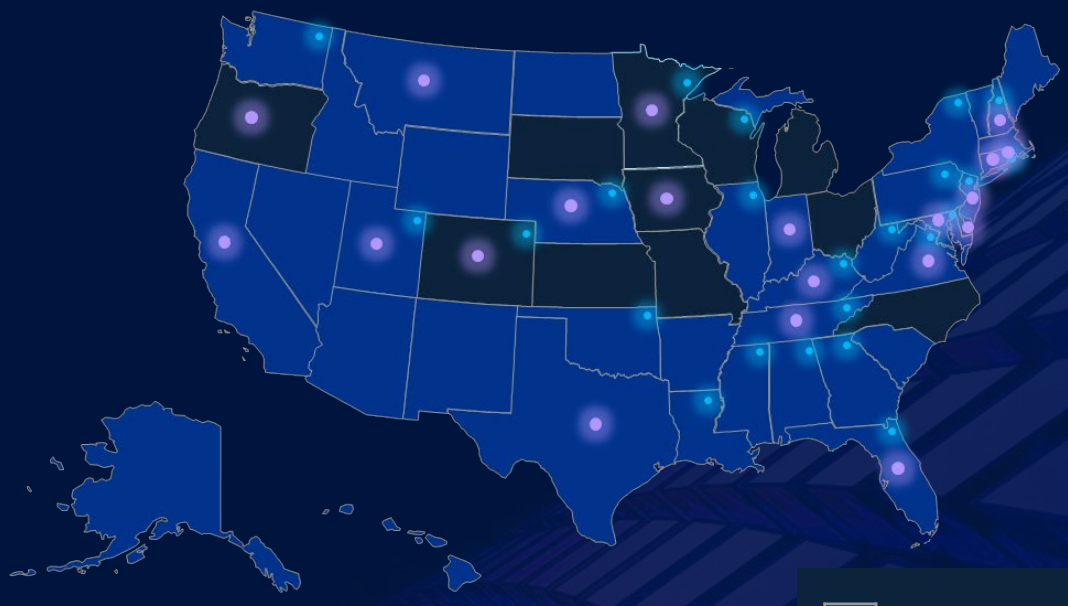
In the 2024 legislative session, more than 850 cyber and privacy bills were introduced across 43 states with 23 states ultimately enacting 47 bills. So far in the current 2025 legislative session, more than 220 cyber and privacy bills have been introduced across 38 states. Many cyber and privacy laws are coupled with AI laws (for which more than 900 bills have been introduced in 2025). The number and varying requirements of these laws greatly increases the complexity of the regulatory environment. As the new Administration has signaled a shift toward "de-regulation", states are likely to expand consumer protections and enforcement within their jurisdictions.

Regulatory signals at the state level will follow state enacted legislation, which includes:

Signals	Description/Examples
Expanding Patchwork of Numerous and Varied Cyber and Privacy Laws	Twenty states have enacted broad privacy laws (7 in 2024) that provide generalized protections for an individual's data, including rights to: • Access, correct, and delete personal data • Opt-out of targeted advertising, profiling, and sale of data Many other states are currently considering such privacy legislation (including GA, HI, MS, NM, PA, and WA)
	A trend in individual privacy bills/laws to include protections related to: • Children/minors, including adolescents (up to 18 years old) • Biometric information and genetic data • Sensitive information (e.g., geolocation) • Health information • Individual rights to contest adverse profiling decisions • Data brokers • Data minimization
	Heightened attention on foundational requirements (alongside the expansion of privacy laws and emerging laws/regulations on AI), including: • Vulnerability/risk assessments • Incident response plans • Notifications/disclosures schedules • Risk-mitigating controls, including multifactor authentication and physical and system monitoring • Business continuity and disaster recovery planning • Affirmative defense for meeting established cybersecurity standards/safeguards for data protection

U.S. State Cyber and Privacy Laws and Regulations

In 2024, more than 20 states enacted cyber/privacy legislation; So far in 2025, more than **220** bills have been introduced in **38** states†



† Derived from Multistate.

For more information, please contact Amy Matsuo, Matt Miller, or Orson Lucas.

Contact

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

Connect on LinkedIn

Learn about us: **kpmg.com**

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.