HINSHAW

Alerts

Hinshaw's 5 Data Privacy Day Regulatory and Litigation Predictions for 2025

January 28, 2025
Privacy, Cyber & AI Decoded

To commemorate Data Privacy Day, we are pleased to outline Hinshaw's top five privacy predictions for 2025. We covered our strategic recommendations for privacy planning in our earlier alert, and today, we provide some additional big-picture guidance to help organizations focus their privacy programs and expenditures in 2025.

1. New state laws on AI, healthcare privacy, children's data, and comprehensive privacy legislation will continue to grow exponentially.

With the lack of a federal privacy bill, in week three of 2025, there are already numerous state legislative bills introduced on:

- artificial intelligence (Connecticut and Texas);
- healthcare privacy (New York);
- controlling access to children's data through age verification (Nebraska);
- comprehensive privacy bills (New York, Massachusetts, Illinois, and Hawaii);
- along with many more bills on the way.

According to RegAlytics, a leading provider of regulatory alerts globally, over 132 artificial intelligence (AI) bills have been introduced in the United States and the District of Columbia as of the start of Data Privacy Day. As a reminder, all comprehensive privacy laws require reasonable security controls, which regulators will enforce after a breach.

2. State attorney generals and regulators will increase their investigations and enforcement of comprehensive privacy and data security laws, especially regarding connected cars.

We have continued to see an increase in state regulatory activity and investigations about the collection, use, transfer, disclosure, sharing, and "sale" of consumer personal information. One repeat investigatory topic by regulators concerns the collection and sharing of driving and other sensitive data collected by automobiles and shared with third parties, such as insurance companies.

Attorneys

Cathy Mulrow-Peattie

Justyna H. Regan, Ph.D.

John P. Ryan

Service Areas

Privacy, Security & Artificial Intelligence

Both parties' regulators have brought these investigations, demonstrating that privacy is a bipartisan issue. We expect that this trend will continue as technology and disclosures in this area are complex.

3. There will be increased class action activity in state privacy cases.

As more states enact privacy statutes, we expect an increase in privacy class actions at the state level. One of the main issues we expect to be argued is whether plaintiffs have standing to assert claims based solely on statutory violations and/or the potential for future harm.

4. There will *not* be a comprehensive federal privacy law this year.

Given the current Trump Administration's political agenda, comprehensive federal privacy and AI legislation are unlikely, especially as last year's failed federal privacy bill showed us there is no Congressional agreement on federal preemption or a private right of action.

We do expect to see Federal Trade Commission ("FTC") regulatory activity on large and egregious cases similar to the Trump One FTC, especially as they relate to data security and national security issues.

National security issues, especially the use of personal data by foreign adversaries, will be top of mind for this presidential administration but they will be counterbalanced again by the practical considerations of many U.S. tech businesses and manufacturers that have operations in China.

5. On the international privacy landscape, there will be continued enforcement against U.S. companies for failing to comply with local laws.

An accelerated surge in new technology developments, such as AI, facial recognition, and biometric data collection, has been drawing scrutiny from the General Data Protection Regulation (GDPR). Therefore, U.S. companies developing or deploying AI solutions may face stricter enforcement under GDPR, especially in the data protection components of automated decision-making, transparency, and data minimization.

Moreover, to date, European Union (EU) data protection authorities (DPAs) have been predominantly focused on large U.S. companies. We believe that may change, and mid-sized and smaller U.S. businesses operating globally may be subject to more enforcement actions, particularly in sectors like e-commerce, SaaS, and cloud services, as DPAs scale their efforts.

What should companies be doing to comply with privacy laws?

With the growing number of engaged state regulators and heightened privacy scrutiny, companies should be preparing for these new and existing laws by taking the following steps to organize their privacy house:

1. Review data and asset mapping;
2. Update privacy and AI policies for ongoing changing legal requirements as they apply to your business;
3. Ensure your business has accurate consent for the use of sensitive data and other personal data;
4. Confirm that your data protection addendums will hold up in court; and
5. Update your company's cybersecurity controls and policies to current standards.