CYBERSECURITY AND DATA PRIVACY

INFORMATION MEMO

JANUARY 29, 2025

What's On the Horizon: Looking Ahead to 2025 Data Privacy Trends and Developments

Last year proved to be an incredibly active year for data privacy legislation, state and federal enforcement actions, and new compliance challenges introduced by emerging technology. Looking ahead to this year, there is no sign of a slowdown. This alert provides a preview of the headline privacy issues and compliance hurdles that organizations across a variety of industries will have to contend with.

1. New State Privacy Laws and Enforcement.

Comprehensive state consumer privacy laws in Delaware, Iowa, Nebraska, New Hampshire and New Jersey will all come into effect in 2025. Organizations that collect and process data from residents of these states will need to determine whether they are subject to these new laws and, if so, carefully evaluate whether their existing data processing practices align with new state law requirements. More states, including New York, are expected to follow suit, which will add another layer of complexity to organizations already subject to the growing patchwork of state consumer privacy laws.

State regulators, particularly in New York, Texas and California will continue to expand privacy and cybersecurity enforcement efforts. While smaller organizations may escape attention from federal regulators like the Federal Trade Commission (FTC), these organizations will need to regularly examine their data governance frameworks to avoid falling within the crosshairs of motivated state regulators in their home states.

2. Federal Privacy and Data Security Trends.

The FTC will continue to focus on unlawful privacy practices, especially to the extent that violations impact children's privacy. While it is not completely clear how the new administration will alter the FTC's policy focus going forward, the protection of children and their data is a bipartisan point of emphasis that will likely continue to be at the forefront of federal privacy enforcement.

Additionally, foreign data transfers, which traditionally have been more of a focus for European regulators, will likely now be a significant focus for federal regulators in the U.S. The Protecting Americans' Data from Foreign Adversaries Act (PADFA), enacted on April 24, 2024, provides the FTC with a powerful new tool to prevent U.S. companies from transferring personally identifiable information to U.S. foreign adversaries, including the People's Republic of China. Given the new administration's emphasis on protecting American interests abroad, PADFA's data transfer restrictions will likely pose new challenges for U.S. companies that rely on international service providers to process data.

3. AI and Privacy.

As artificial intelligence (AI) tools, and particularly generative AI, continues to aggressively permeate the health care, manufacturing, education and service industries, new compliance obligations will likely follow. Issues pertaining to consumer consent, protection of personal autonomy and responsible use of AI tools will loom large as more and more organizations seek to reap the benefits of automation.

The new administration has already expressed a strong interest in increasing the accessibility of AI tools available to the public. Indeed, the new administration has publicly admonished the Biden Administration's efforts to regulate AI development as "unnecessarily burdensome" and a threat to American innovation and leadership in the technology sector. Federal support for unfettered AI development and use will likely prompt many states to introduce legislation aimed at protecting the privacy and individual rights of their residents.

Across the pond, all eyes will be on the enforcement of the EU AI Act. The Act is a first of its kind, trailblazing regulation that primarily imposes use restrictions and disclosure requirements on AI developers, the extent of which depends on the risks an AI tool poses to consumers' privacy and individual rights. Much like the GDPR's significant influence on U.S. state consumer privacy laws, the EU AI act is expected to inspire similar legislation in the U.S.

4. Biometric Data.

As more U.S. organizations adopt the use of biometric technology for practical applications like physical and IT access controls, identify verification and timekeeping purposes, the collection of biometric data will continue to be heavily scrutinized. Due to Illinois' Biometric Privacy Act's (BIPA) broad extraterritorial reach and private right of action, BIPA is expected to remain a hotbed for consumer protection litigation.

Other states, such as Texas and Washington also have standalone biometric privacy laws and many comprehensive state consumer privacy laws classify biometric data as "sensitive information," subject to more stringent compliance requirements. More states are expected to follow suit. Organizations collecting biometric data will need to carefully comply with notice, consent, processing and retention requirements to avoid regulatory enforcement and consumer class action exposure.

5. Health Data Privacy.

Recently enacted health data privacy laws in Connecticut, Nevada and Washington provide consumer privacy protections beyond the narrow purview of the Health Insurance Portability and Privacy Act (HIPPA). Earlier this year, New York lawmakers passed the New York Health Information Privacy Act, which, if signed by Governor Hochul will impose stringent health data processing restrictions on organizations not traditionally considered a covered entity under HIPAA and grant powerful consumer rights to New York residents.

6. Privacy Litigation.

As the body of U.S. state privacy laws expands, privacy-related litigation is expected to increase as well. Large data breaches that garner national attention are frequently litigated and we expect data breach litigation to remain at the forefront in 2025. Notably, a singular data breach can lead to multiple legal actions depending on the scope of impacted individuals and severity of the compromise. The recent PowerSchool breach, which exposed thousands of student and educator records, is a great example of how one security incident can result in multiple, simultaneous class action suits.

Further, consumer-focused advocacy groups continue to scrutinize website data collection practices, privacy policy disclosures and the use of AI chatbots that interact with website users. Consumer-facing organizations will need to regularly review their website privacy polices and business activities in each state to make sure they are compliant with new laws and to ensure public disclosures reflect their actual data processing practices.

Key Takeaways

It is clear that both state and federal authorities will continue to prioritize consumer privacy safeguards in the coming year. The introduction of new laws, increased enforcement and the unpredictable trajectory of AI technology will all pose significant challenges for organizations in every industry. Organizations should examine their exposure to both new and persistent privacy compliance hurdles by considering the following:

- State Law Exposure. Conduct an analysis of business activities in each state with active consumer privacy laws. Many state laws have revenue and data processing thresholds that determine which organizations must comply. These thresholds are subject to change, forcing organizations to routinely evaluate their exposure to these laws.
- Children's Privacy. Organizations that allow children to access products and services online must exercise care when interacting with minors. Inadequate or nonexistent parent/guardian consent mechanisms are likely to attract regulatory attention. Websites that are not intended for children should clearly state this in a website privacy policy.
- Embrace AI, With Caution. There is no denying that AI is here to stay and avoiding it all together will put any organization at an immediate competitive disadvantage. Still, blindly adopting AI tools without sound policy governing use will expose organizations to privacy-related litigation and enforcement actions.
- Revisit Your Privacy Framework. Organizations will need to continue to evaluate and update internal data governance documents (e.g. IT security policies, employee acceptable use polices and incident response plans) to ensure they remain compliant with new laws and regulations. Special attention must be paid to external polices (e.g. website privacy policies, terms of use, HIPAA Notices of Privacy Practices), as errors and inaccurate representations provide potential litigants with a strong foothold to bring class action lawsuits.

Bond's cybersecurity and data privacy team routinely assists organizations with navigating state and federal privacy compliance obligations. For more information or guidance concerning any of the topics above, please contact Jessica L. Copeland, Mario F. Ayoub or any Bond attorneys in the cybersecurity and data privacy practice.

BOND SCHOENECK & KING ATTORNEYS