wiley

ALERT

10 Key Privacy Developments and Trends to Watch in 2025

January 9, 2025

As we enter the New Year, Wiley is looking ahead to the top privacy developments and trends to watch in 2025. On the state side, 2025 kicked off with several new privacy laws going into effect in January, and states continue ramping up enforcement activities. At the federal level, privacy issues will likely remain a focus, particularly in the area of sensitive personal data, even if priorities shift in a new Administration. In addition to new laws and regulation, private litigation is expected to continue in certain key areas, and an expected upturn in transactions will make privacy-related due diligence critical.

Below, we identify 10 privacy issues to watch this year.

1. New State Privacy Laws Are Effective and Are Being Enforced.

The wave of state privacy laws is continuing this year. In addition to eight laws that became effective in recent years, five new comprehensive state privacy laws take effect this month in Delaware, Iowa, Nebraska, New Hampshire, and New Jersey. Comprehensive privacy laws in Minnesota and Tennessee will take effect in July 2025, and Maryland's Online Data Protection Act takes effect on October 1, 2025. All said, by the end of this year, the number of comprehensive state privacy laws in force will grow to 16.

With the patchwork of comprehensive state privacy laws continuing to grow, many companies have moved towards a "nationwide approach," adopting compliance plans that build on the commonalities and account for the outlier provisions among the laws. However, there are differences that complicate compliance, including the scope of exceptions and treatment of sensitive data. The

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Stephen J. Conley
Associate
202.719.4572
sconley@wiley.law

Lauren N. Lerman
Associate
202.719.4664
llerman@wiley.law

Alissa Lynwood
Associate
202.719.4527
alynwood@wiley.law

Kelly Laughlin
Associate
202.719.4666
klaughlin@wiley.law

Stephanie Rigizadeh
Associate
202.719.4736
srigizadeh@wiley.law

Practice Areas

Artificial Intelligence (AI)

FTC and Consumer Protection

Privacy and Cybersecurity Litigation and

Maryland law in particular has stricter data minimization and sensitive personal data provisions than seen in other laws.

At the same time, state enforcers, including the California Privacy Protection Agency and state Attorney General offices, are ramping up inquiries and enforcement actions. These actions are not following the traditional "multi-state" approach to consumer protection investigations and instead have been turning on unique aspects of state privacy law. Texas, in particular, has been actively enforcing its new privacy laws. The Texas Data Privacy and Security Act has a 30-day cure period, which is beneficial for companies, but makes it critical for companies to respond quickly to any notice of apparent violation by the Texas AG's office.

2. The Federal Trade Commission (FTC) Will Continue to Look at Privacy Practices, Including on Children's Privacy.

President-Elect Trump has announced that current FTC Commissioner Andrew Ferguson will be named Chair. Commissioner Ferguson is likely to steer the Commission back to a case-by-case enforcement approach, rather than attempting to enact broad privacy rules. For example, during the Biden Administration, the FTC began considering whether to adopt broad privacy rules, releasing a wide-ranging advance notice of proposed rulemaking (ANPR) about "commercial surveillance" and data security in August 2022. That ANPR never moved forward to a proposed rule, and Commissioner Ferguson has been critical of this kind of rulemaking and has cautioned against excessive regulation and legal theories that he thinks go beyond the bounds of the FTC Act and the agency's authority. At the same time, he is still supportive of the FTC bringing privacy-related cases under the FTC's existing statutory authority.

While the FTC's privacy enforcement authority priorities may shift in the new Administration, children's privacy may remain a priority as the FTC continues to evaluate how to move forward on a December 2023 notice of proposed rulemaking (NPRM) proposing revisions to its Children's Online Privacy Protection Rule. Commissioner Ferguson has also been critical of "big tech" practices and raised issues with content moderation practices. Overall, companies should continue to monitor FTC enforcement trends and priorities.

3. Biometrics Practices Continue to Be Scrutinized.

The collection and use of biometric data will continue to be scrutinized – both in litigation and by enforcement agencies. Over the last decade, a large number of biometric privacy class action lawsuits have been brought under the Illinois Biometric Information Privacy Act (BIPA), and similar litigation is likely to continue. However, companies should also pay attention to other state laws, outside of Illinois, that strictly regulate the collection of biometric data. These include the Texas Capture or Use of Biometric Identifier Act, the Washington Biometric Privacy Protection Act and My Health My Data Act, and comprehensive state laws that classify biometric data as "sensitive." Key issues include whether businesses (1) obtain proper consent before collecting biometric data from consumers, (2) provide adequate notice to consumers about how their data would be used and stored, and (3) comply with data retention requirements. With the increasing use of biometric data for purposes that range from security and authentication to health monitoring and AI analytics, companies should take stock of their current biometric data practices and review for compliance.

4. Health Data Laws Are Effective and May Be Interpreted Broadly.

Connecticut, Nevada, and Washington state all have implemented comprehensive consumer health privacy laws that could portend an increase in enforcement actions in 2025. The Washington My Health Data Act has the broadest scope of the three, defining "consumer health data" to include "personal information that is linked or reasonably linked to a consumer and that identifies a consumer's past, present or future physical or mental health status" as well as other categories such as "[p]recise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies." And as explained by the Washington Attorney General's Office, "consumer health data" could also encompass inferences drawn from *nonhealth* data when that information is used by an entity to associate or identify a consumer with consumer health data. The Nevada health data law, on the other hand, provides a more tailored definition of "consumer health data" as "personally identifiable information that is linked or reasonably capable of being linked to a consumer and that a regulated entity *uses* to identify the past, present or future health status of the consumer." The Connecticut Data Privacy Act's definition of "consumer health data" follows Nevada, also requiring that controllers actually *use* such data to identify a consumer's physical or mental health condition or diagnosis.

Notably, the Washington law provides consumers with a private right of action for consumer health data-related violations, while the other laws only allow for regulator enforcement. Companies should watch for an uptick in consumer health data lawsuits and be sure that their compliance strategies track the breadth of the laws.

Additionally, a number of 2024 health privacy proposals could reemerge in 2025, such as the Vermont My Health My Data Law, which almost passed in 2024.

5. Data Brokers Will Continue to Face Scrutiny from Regulators.

Data brokers faced scrutiny from regulators at the federal and state level in 2024, and this focus is expected to continue in 2025. For example, in December 2024, the FTC settled with two data brokers over allegations that the companies collected, retained, and sold consumers' precise location data associated with "sensitive" locations without adequately verifying consumers' consent. Certain states have similarly demonstrated a focus on enforcing new state laws covering data brokers. Texas' data broker registration law went into effect in March 2024 – and in June 2024, the Texas Attorney General's Office sent letters to more than 100 companies, notifying them that they were required to register as a data broker with the Texas Secretary of State. In December 2024, the Texas AG followed up those letters with six violation notices sent to companies that had still failed to register in accordance with the Texas law. The California Privacy Protection Agency (CPPA) similarly issued enforcement actions against two companies in November 2024 that failed to register as data brokers in the state of California. These federal and state enforcement actions against data brokers at the end of 2024 are a strong indicator of what may come in 2025. Of note, data broker laws and enforcement efforts can impact companies that do business with data brokers – either in providing or receiving data – not just the brokers themselves.

6. New Federal Restrictions on Foreign Personal Data Sales Will Become Effective.

Personal data sales or other personal data transactions outside the United States will be subject to additional restrictions and requirements in 2025. First, significant requirements were enacted in 2024 with the passage of the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA). Enforced by the FTC, PADFA prohibits "data brokers" from selling, licensing, or transferring for consideration an American's "personally identifiable sensitive data" to certain "foreign adversary" countries – China, North Korea, Russia, and Iran – or to any entity "controlled" by those foreign adversary countries. Specifically, PADFA applies to sensitive data sales to entities with more than 20% or more ownership by an individual or business domiciled or with a principal place of business in a foreign adversary country. The law went into effect in June 2024.

Second, and adding to PADFA, at the very end of 2024, the U.S. Department of Justice (DOJ) issued a final rule that will restrict and/or regulate additional foreign personal data transactions. That rule broadly restricts and, in certain circumstances, prohibits U.S. persons from entering into certain transactions (e.g., data brokerage, vendor agreements, employment agreements, and investment agreements) with countries of concern or entities associated with those countries, to the extent that such covered transactions involve bulk U.S. sensitive personal data (defined to include precise geolocation data, biometric identifiers, personal health data, and personal financial data, among other categories) or government-related data. The DOJ final rule includes civil penalties as well as criminal fines and penalties for willful violations and will become effective on April, 8 2025.

For both laws, companies should implement compliance strategies and monitor enforcement activity and agency guidance.

7. New Texting and Calling Rules Under TCPA Are Coming Online in 2025, Raising Enforcement and Litigation Risks.

Two new sets of Telephone Consumer Protection Act (TCPA) rules related to outbound calls and text messages are set to take effect in 2025 – the one-to-one consent rule for obtaining prior express written consent (effective January 27, 2025) and new rules for honoring consumer opt-out requests (effective April 11, 2025). The TCPA's rules require that callers obtain prior express consent for calls to wireless numbers that use autodialers or artificial or prerecorded voices, and for calls to residential landlines that use prerecorded or artificial voices. Once effective, the Federal Communication Commission's (FCC) new one-to-one consent requirement will obligate parties making telemarketing calls using an automatic telephone dialing system or an artificial or prerecorded voice to obtain prior express written consent "one seller at a time." Additionally, the consent given must be in response to a disclosure to the consumer that is "clear and conspicuous," and the content of the calls and/or texts sent to the consumer must be "logically and topically associated with" the website where the consumer gave consent.

The FCC's new opt-out requirements, among other things, codify certain consumer opt-out attempts as *per se* reasonable that calling parties must honor, and require calling parties to honor revocations made in any reasonable manner within 10 business days. It also clarifies that "when consent is revoked in any reasonable manner, that revocation extends to both robocalls and robotexts regardless of the medium used to communicate the revocation of consent."

Companies engaged in outbound calling and texting should assess their current TCPA compliance plans and disclosures to evaluate whether changes need to be made to comply with the new consent disclosure and opt-out requirements. For years, the TCPA has been the source of widespread litigation, due to the law's private right of action and statutory damages. These litigation trends are not expected to slow in in 2025.

8. New State AI Laws Can Impact How Companies Handle Personal Data.

States have been at the forefront of considering AI-related legislation, and last year, Colorado became the first state to adopt a broad AI law – the Colorado Anti-Discrimination in AI Law (Colorado ADAI). The law goes into effect in February 2026 and broadly establishes requirements for developers and deployers of "high-risk artificial intelligence systems," as well as disclosure requirements for AI systems that are intended to interact with consumers. This adds to Colorado's already-existing privacy law and regulation of certain automated decisions that involve the use of personal data.

In 2025, more regulation, proposed legislation, and enforcement activity is expected. For example, important rulemaking activity is already underway in California, as the CPPA is accepting comments on proposed rules governing automated decision-making technology (ADMT) through January 14, 2025. And Colorado is expected to launch its rulemaking activity – authorized by the new Colorado ADAI – in advance of that law going into effect in early 2026. State legislatures around the country are poised to consider additional bills that might regulate AI. For example, a bill that would regulate certain uses of AI has already been introduced in Texas. These proposals have the potential to impact companies' privacy and data governance practices more broadly, and are important to watch as 2025 advances. Finally, states are expected to scrutinize AI uses through increased enforcement activity as well. For example, in December 2024, the Oregon AG issued guidance explaining that Oregon's "Unlawful Trade Practices Act, Consumer Privacy Act, and Equality Act,

among others, all have roles to play [in regulating AI]."

9. Privacy Litigation on Website Data Collection Practices Will Continue.

In 2024, the number of data privacy-related lawsuits continued to skyrocket, with no signs of slowing in the new year. In 2024 alone, federal courts saw over 1,970 data privacy lawsuits, and many other cases have been filed in state courts.[1] Many of these cases involve challenges to use of website technologies. For example, numerous cases have alleged that interactive chat functions on websites impermissibly access consumer conversations with website operators, in violation of the California Invasion of Privacy Act (CIPA) or other state statutes. Other cases allege that companies violated CIPA by installing an impermissible "pen register" on user devices and collecting user personal data without authorization. And another line of lawsuits involves claims that website pixels capture and transmit health data to third parties in an attempt to bolster targeted advertising practices.

While these novel legal theories continue to be litigated, companies face uncertainty as to whether certain website data collection practices could be subject to class action litigation. In addition to ensuring compliance with the comprehensive state privacy laws, companies should take a close look at website chat, data collection, and pixel practices, particularly if they may be dealing with sensitive user data (such as health or financial data).

10. Transactional Diligence on Privacy Will Be Critical.

With the incoming Trump Administration expected to be more friendly towards transactional activity, diligence on privacy and data governance risks – including those outlined above – will be critical. Companies contemplating a merger, acquisition, joint venture, or other transaction involving another company that collects, uses, or shares consumer data should perform due diligence on privacy practices. In many cases, it will be important to look ahead to how regulations may evolve on the federal, state, and international level to determine whether and how data involved in the transaction can be used going forward, and to implement procedures to mitigate compliance risk.

***

Wiley's Privacy, Cyber & Data Governance team assists clients with a full spectrum of privacy, cybersecurity, and data governance issues, which includes compliance, advocacy, and successful representation in litigation and investigations. Please reach out to any of the authors with questions.

[1] Westlaw Litigation Analytics: Data Privacy Analytics (last visited December 31, 2024).