wiley

ALERT

Five Privacy Checkpoints to Start 2026

January 6, 2026

As 2026 kicks off, new state privacy laws and amendments are coming into effect, the stream of privacy litigation continues to ramp up, and new AI and other data-driven technology is knocking on the door. Federal and state privacy enforcers have spent 2025 signaling that they will be active in 2026. Here we outline five areas that in-house privacy and compliance professionals should watch as the new year kicks off – all areas where we expect greater activity in 2026.

Below we cover:

- The impact of new AI tools on privacy compliance
- Managing website technology risks given litigation trends
- Handling sensitive data including health and geolocation information
- Approaching kids' data, even for websites and services not directed to kids
- Dealing with foreign transfers of personal data and extensive new rules that may be applicable

****

1. **Implementing AI tools will impact privacy compliance.** New AI tools can provide substantial benefits for companies, but privacy compliance should be built into consideration and implementation of AI tools. For example, companies may use AI tools to read and summarize a wide range of complex data and documents, which implicates privacy controls on personal data that might be accessed by the tool. Personal data use and sharing – regardless of the technologies or tools used – is subject to your company's applicable privacy policies, and some personal data may be subject to various

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Practice Areas

Advertising Technology (AdTech) Data Privacy and Consumer Protection

FTC and Consumer Protection

Privacy, Cyber & Data Governance

State Privacy Laws

state and federal privacy statutes, including the newly finalized CCPA rules related to automated decision-making technology (ADMT). These considerations are particularly important when using third-party services that might seek rights to keep or use data for model training purposes, and the risks are particularly heightened when using AI chatbots to interact with individuals.

2. **Website technologies are in the spotlight.** A recent flood of class action demand letters and filings have advanced novel theories as to how common website technologies – like third-party analytics and social media pixels – could violate pre-internet laws like the California Invasion of Privacy Act (CIPA). Companies should review their website data collection practices and disclosures to assess and address risks and compliance obligations in this area, including reviewing what their cookie banners say and how their website works.
3. **Sensitive data like health and geolocation information should be carefully handled.** Sensitive personal data is often subject to heightened requirements under state laws, and states enforcers have shown that they are particularly interested in health data and precise geolocation data, as well as kids' data (discussed below). The new Maryland privacy law (effective October 2025) even includes a ban on the sale of sensitive personal data including precise geolocation data and health data, and the definition of a "sale" can be interpreted broadly. Companies dealing with biometrics should be sure to comply with laws that may impose consent and other requirements, such as Illinois' long-standing Biometric Information Privacy Act (BIPA) and Colorado's heightened protections for biometric data, which took effect in 2025.
4. **Companies must pay closer attention to kids' data.** While companies that have directed their services to children under 13 are well-accustomed to privacy requirements under the Children's Online Privacy Protection Act (COPPA), the most recent changes are worth further review, particularly as the Federal Trade Commission (FTC) has emphasized COPPA enforcement as a priority. Additionally, legislators and regulators are now increasingly interested in imposing age gating (or "age assurance") requirements, which would require adoption of technologies that would result in websites or apps receiving the *actual age* of individual users. While one state age assurance law in Texas was enjoined in late December – just over a week before its effective date – others are scheduled to become effective later this year if not also blocked. In parallel, the FTC is holding a January workshop on online age verification technologies and has promoted the use of such technologies in certain contexts. Regardless of whether it is due to a statutory requirement or a voluntary practice, companies that receive information that any personal data is associated with a child under 13 – or under 16 in some states – should closely consider the additional federal and state privacy requirements that may apply.
5. **Foreign transfers of personal data are now subject to substantial regulation.** The U.S. Department of Justice's (DOJ) Data Security Program Rule went into effect last year, and it imposes strict requirements on transfers of certain "sensitive" personal data outside of the United States. The Rule potentially covers data that ranges from precise geolocation data to device identification information to health data. The Rule is targeted at transfers to countries of concern (e.g., China) and certain covered persons, but it also imposes contractual and other requirements even when covered data is

transferred to any non-U.S. person. The DOJ can enforce the law through both civil and criminal penalties, further raising the stakes for companies handling personal data across national borders. Similarly, the FTC has signaled a focus on enforcing the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA) – a law that took effect in mid-2024 and that prohibits certain sales of personally identifiable sensitive data to specified foreign adversary countries, or any entities controlled by a foreign adversary country.

Overall, more comprehensive state privacy laws and amendments will come into effect in 2026, and companies subject to specific regulations – like data broker regulations – will have further requirements as well. And these privacy requirements will come on top of new and existing cybersecurity and AI-specific requirements. These five checkpoints should serve as a starting point for evaluating privacy compliance in the new year.

***

Wiley's Privacy, Cyber & Data Governance team has broad experience in navigating compliance issues around cutting-edge technology and the evolving legal landscape, and handling enforcement and litigation matters. For questions about this alert, please contact the authors.