Proskauer

Proskauer on Privacy: 2024 Reflections & 2025 Predictions

Proskauer on Privacy on **March 17, 2025**

2024 marked another significant year for privacy law, with new state legislation and high-stakes litigation reshaping the landscape. Legal battles over tracking technologies, biometric data, and children's privacy intensified, while federal agencies, including the Federal Trade Commission ("FTC") and the U.S. Department of Health and Human Services Office for Civil Rights ("HHS OCR"), ramped up their efforts through major enforcement actions and high-profile settlements, marking a new era of increased accountability.

Federal Privacy Law Gridlock

Attempts to pass comprehensive federal privacy legislation in 2024 fell short once again, leaving a significant gap in U.S. data protection standards and a lack of a national data privacy standard. Despite bipartisan support, the American Privacy Rights Act ("APRA"), designed to unify privacy laws, preempt conflicting state regulations, introduce a private right of action, and enforce opt-out mechanisms, did not pass the 118th Congress. Still, the last Congress passed, as part of a larger appropriations bill, the "Protecting Americans' Data from Foreign Adversaries Act of 2024" (15 U.S.C. § 9901), which makes it unlawful for a data broker "to sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available personally identifiable sensitive data of a United States individual to (1) any foreign adversary country; or (2) any entity that is controlled by a foreign adversary." Without a comprehensive federal privacy law, states were forced to fill the void by passing their own. But each state that did so had independent and distinct requirements for those laws, leading to burdensome compliance efforts, higher operational costs, and increased legal risks for businesses.

FTC Rulemaking and Enforcement Intensifies

In 2024, the FTC prioritized safeguarding sensitive data, focusing on location tracking, health data, children's privacy, and cybersecurity. The agency secured key settlements, banning the sale of sensitive location data without consent or deidentification, investigating health data misuse, and filing a Children's Online Privacy Protection Act ("COPPA") action against TikTok. In terms of children's privacy, it should also be noted that at the close of the Biden administration, the FTC finalized changes to the COPPA Rule to set new requirements surrounding the collection, use and disclosure of children's personal information, including requiring covered websites and online service operators to obtain opt-in consent from parents for targeted advertising and other disclosures to third parties.

One notable FTC settlement prohibited a data broker from selling or sharing sensitive location data after it was collected and distributed without adequate safeguards. Another targeted a cybersecurity company accused of unlawfully selling browser data and engaging in deceptive practices. The FTC also filed complaints and secured proposed settlements with an alcohol addiction treatment service and a mental health telehealth company, alleging they illegally shared users' health information for advertising purposes through third-party tracking tools.

The agency also intensified its focus on deceptive and fraudulent claims surrounding AI products and services. Companies using AI-driven platforms were also urged to take "necessary steps to prevent harm before and after deploying [an AI] product" to ensure fairness, minimize bias, and comply with evolving regulatory standards. As the FTC expanded enforcement in this area, businesses faced growing pressure to proactively mitigate risks and implement safeguards to avoid costly investigations and penalties.

HIPAA Enforcement and Judicial Constraints

In 2024, the HHS OCR focused heavily on enforcing the Health Insurance Portability and Accountability Act ("HIPAA"), concluding over 22 enforcement actions. However, the landmark ruling in *American Hospital Association v. Becerra* curtailed HHS's authority over online tracking liability under HIPAA, holding that HHS could only regulate information that both identifies an individual and directly relates to their health.

Following the ruling, HHS voluntarily withdrew its appeal, signaling a shift in its approach to online tracking and privacy enforcement. The decision marked a critical limitation on HHS's ability to regulate digital health technologies and underscored the ongoing tension between evolving digital practices and traditional privacy regulations.

Litigation Trends: Old Laws, Modern Issues

With no federal privacy law in place, plaintiffs in 2024 relied heavily on old electronic privacy statutes for class action lawsuits, including the Video Privacy Protection Act of 1988 ("VPPA"), Electronic Communications Privacy Act of 1986 ("ECPA"), and numerous state laws, such as California's Invasion of Privacy Act of 1967 ("CIPA") and Song Beverly Credit Card Act of 1971 ("SCCA"), to address modern online privacy concerns.

While VPPA was designed to prevent video rental stores (e.g., Blockbuster) from sharing customers' personal data and the ECPA and CIPA to prevent eavesdropping and traditional wiretapping, plaintiffs have recently repurposed these laws to target alleged misuse of internet technologies such as cookies, pixels, chatbots, and session replay technology, a trend that continued to gain traction throughout 2024. Plaintiffs have also attacked the use of these technologies using the SCCA—a statute that restricts businesses from collecting unnecessary personal identification information during credit card transactions. While originally intended for brick-and-mortar retailers, plaintiffs are now extending the statute's application to digital commerce, limiting how businesses can request and store consumer data during online purchases.

Class action lawsuits over data breaches and mishandled opt-out requests also continued to surge, fueled by regulatory developments and high-profile breaches. Data subject requests for deletion, access, and opt-outs increased by 246% between 2021 and 2023, highlighting the demand for transparency and control. A 2024 audit found 75% of businesses failed to honor opt-out requests, highlighting the practical challenges of data privacy compliance.

To mitigate their legal privacy risks, companies will need to consider refining consent mechanisms, implementing robust consent management platforms, and exploring alternatives to cookie-based or pixel tracking. Compliance with all of these laws are critical to ensure proper disclosures, limit personal data requests, and reinforce consumer trust.

Comprehensive State Privacy Laws

In 2024, seven states enacted comprehensive privacy laws in 2024 – raising the total number of comprehensive state privacy laws to 20. Many of these laws, including Florida, Montana, Oregon, and Texas, went into effect in 2024 – Nebraska, New Hampshire, Delaware, Iowa, and New Jersey – went into effect at the beginning of 2025, Minnesota, Tennessee and Maryland will go into effect later in the year (i.e., July 2025 and October 2025 respectively). Kentucky, Rhode Island and Indiana are scheduled to go into effect in 2026.

State-level enforcement also intensified, with California, Texas, and New Hampshire leading major efforts. For example, California reached a settlement with DoorDash in February 2024 after the company purportedly sold its California customers' personal information without providing notice or an opportunity to opt out in violation of the California Consumer Privacy Act ("CCPA") and CalOPPA. In June 2024, the state reached another settlement with Tilting Point Media for violations of CCPA and COPPA for Tilting Point's alleged collection and sharing children's data without parental consent.

In addition, Texas reached several major settlements, two of which involved Meta and the company's purported violations of biometric privacy laws, and a first of a kind settlement involving a Dallas based artificial intelligence healthcare tech company for alleged deceptive generative AI practices. The state also initiated a new suit against General Motors in August 2024 for unlawful sale of driving data, and announced an investigation into fifteen companies for potential violations of Texas' Securing Children Online through Parental Empowerment Act and Data Privacy and Security Act.

2025 Privacy Predictions

2025 is expected to be another defining year for privacy regulation, with key trends from recent years continuing to evolve and present new challenges for businesses. The fragmentation of state-level privacy laws, increased enforcement, and the rapid evolution of rules governing biometric data and AI technologies are expected to intensify.

Businesses can expect heightened scrutiny on algorithmic transparency, and biometric protections. Generative AI is also expected to draw significant regulatory attention as the technology matures and states continue to consider additional legislation or regulations, whether it be related to marketing claims, employment, transparency, AI deepfakes, or publicity rights. Companies in health, finance, and technology, specifically, should remain vigilant as regulators push for stricter accountability. While compliance challenges and rising operational costs are likely, organizations that proactively audit data-sharing practices, update privacy policies, and ensure AI compliance will be equipped to navigate the evolving regulatory landscape and reduce overall legal risks.

Federal Legislative Efforts Still Struggle

Despite a growing appetite for a unified privacy framework, progress remains slow heading into 2025. The inability to advance the APRA in 2024 underscores the challenge of balancing state autonomy with uniform, national standards. These challenges are only further compounded by the Trump administration's emphasis on deregulation and a heavily divided Congress. Businesses will likely continue operating without a comprehensive federal privacy law for the foreseeable future. However, renewed lobbying efforts, Congressional hearings, and mounting industry pressure suggest that the core concepts undergirding the APRA could reemerge with modifications. Moreover, it is conceivable Congress could pass legislation strengthening children's privacy, given that the Senate overwhelmingly, with a 91-3 vote, passed legislation that included the Kids Online Safety Act and the Teen's Online Privacy Protection Act (collectively known as COPPA 2.0); the legislation later died in the House, but it will likely be taken up again in the current session of Congress.

In the absence of clear federal guidance, businesses should expect to rely on recognized industry standards in the interim. While these standards are instructive, businesses should note that strict adherence to them may not ensure compliance with the complex web of multi-state regulations. Companies operating across multiple jurisdictions should be sure to consult legal counsel as they navigate the current patchwork of privacy laws to reduce their legal risk.

More States Join the Privacy Landscape. With More to Come?

In 2025, several state privacy laws have recently gone into effect and more are set to take effect later in the year, including Delaware, Iowa, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, and Tennessee. These comprehensive privacy laws significantly expand state-level data protection regulations bringing the total number of states with privacy laws to 20. In addition, other states have lifted the data privacy law template and are debating similar bills of their own in 2025 (e.g., New York S365B), and have debated other bills related to consumer health privacy (e.g., New York Health Information Privacy Act, awaiting the governor's signature), social media restrictions and other data privacy related issues.

With compliance becoming more complex, investments in automated tools to monitor regional legal variations are expected to grow, as businesses recognize them as critical for long-term regulatory resilience in an ever-changing environment.

Litigation Trends: Internet Tracking Technologies & Healthcare Data

Regulators and plaintiffs continue to focus on cases involving internet tracking technologies, particularly under statutes including VPPA, ECPA (and state wiretapping laws), and CIPA, as well as laws governing the general collection of website user information, such as the SCCA. These cases increasingly scrutinize how companies track, collect, and use consumer data, particularly in sensitive contexts such as healthcare and wellness.

Against this backdrop, Washington's My Health My Data Act ("MHMDA") which went into effect in 2024, imposes strict privacy protections on consumer health data, extending beyond traditional healthcare providers to include wellness apps, online health services, and companies handling health-related consumer information. The law requires businesses to obtain explicit consent before collecting or sharing health data, maintain transparent privacy policies, and enforce stringent security measures to prevent unauthorized access or misuse.

Notably, the first lawsuit under MHMDA was recently filed against Amazon, marking a significant test case for the law's enforcement. Given the evolving regulatory landscape, businesses should closely monitor litigation and compliance developments in this space.

Continued Momentum for AI, Biometric and Neural Data

Neural data has become a significant privacy concern with the rapid growth of wearable devices and brain-computer interfaces. In 2024, California and Colorado amended their privacy laws to extend protections to neural data, sparking broader regulatory interest and prompting advocacy groups to push for ethical standards and stricter consent requirements. Companies developing neural data technologies, including VR applications, brainwave monitoring devices, and other wearables, are investing in advanced encryption, secure storage, and anonymization methods to safeguard this highly sensitive information.

AI also remains a key driver of both cybersecurity advancements and emerging risks in 2025. In response to privacy violations linked to AI-powered tracking in 2024, businesses are increasingly deploying AI tools to improve threat detection, monitor compliance, and secure sensitive data. Cybercriminals have also embraced AI, using it to execute more targeted and complex attacks, such as deepfake impersonation, advanced phishing schemes, automated network breaches, and large-scale data theft.

As AI adoption grows, companies face rising legal and regulatory risks. To address these challenges, businesses should consider comprehensive AI governance frameworks, including regular algorithm audits, bias detection systems, and accountability structures to meet regulatory standards and maintain consumer trust and a high-quality standard of work.

Conclusion

The transition from 2024 to 2025 marks another important moment in the privacy landscape, with escalating state regulatory demands and stricter enforcement reshaping business practices. Companies must embed privacy into their core operations. By investing in privacy-by-design frameworks, adaptive compliance systems, and monitoring of emerging risks, businesses can stay ahead of shifting regulations. Those that anticipate change, take decisive action, and prioritize reasonable data protection as a competitive advantage will not only reduce risks but position themselves as leaders in an era where privacy drives both trust and innovation.

View original.

Related Professionals

David Fioccola

Partner

Aaron M. Francis

Associate

Anna Chan

Associate

Courtland Cuevas

Associate