5 Privacy Law Trends That Will Continue In 2025

By **Liisa Thomas and Kathryn Smith** (January 9, 2025)

Liisa Thomas

Kathryn Smith

Much changed in the world in 2024. That holds true for privacy developments as well. We expect several developments from 2024 to carry over into 2025, and we outline five in this article: namely, developments in the realm of artificial intelligence, passive data collection, combining data from multiple sources, privacy program expectations, and managing vendors.

Companies will want to keep these five in mind as they prepare their privacy programs for 2025.

1. Ongoing Passage of AI Laws, With Continued Scrutiny Under Deception Theories

We begin our look at upcoming developments with the topic that has been on everyone's mind: AI.

2024 saw much regulatory activity in this space — in the U.S. alone, almost 700 AI-related state bills were introduced. Only a handful were passed into law. Of these, several are standouts that companies should keep in mind.

Both Colorado and the European Union passed comprehensive AI laws. Portions of the EU law go into effect February 2025, while the Colorado law will go into effect February 2026. They generally relate to algorithmic discrimination, and transparency and risk mitigation measures, among other things.

More narrowly, Illinois updated its employment law, H.B. 3773, to prohibit discriminatory uses of AI by employers, with the law's obligations set to take effect January 2026. In March, Utah passed the Artificial Intelligence Policy Act, which requires confirming to a consumer, if asked, that they are interacting with AI. This law is unlike California's similar chatbot law, which requires an affirmative disclosure — the Artificial Intelligence Policy Act — which went into effect May 1, 2024.

In addition to regulatory action, the Federal Trade Commission also took aim at several companies in September with its "Operation AI Comply" enforcement campaign, using theories of unfairness and deception under Section 5 of the FTC Act.

What can companies do to address these legal requirements and minimize risk in 2025?

First, keep in mind that while several of the laws passed in 2024 do not go into effect until 2026, their obligations can be burdensome. It will be wise to use 2025 to begin to prepare. Second, expect that more U.S. states and countries worldwide will pass laws that look similar to the laws that are on the books. Third, keep in mind that while there may be uncertainty about enforcement and legislative direction at a federal level, states have been — and likely will continue to be — active in the space. And finally, fourth, keep in mind the laws' requirements.

The laws' requirements include concepts like transparency — letting people know if they are

interacting with AI, disclosing that information will be used to train AI models, or sharing if AI tools have been used to make significant decisions.

Also required under many of these laws are requirements to minimize discrimination and risk mitigation. Colorado points to the National Institute of Standards and Technology Risk Management Framework, which was updated in 2024, for guidance.

2. Passive Data Collection

There has been a trend over the past several years of plaintiffs class action attorneys scrutinizing passive digital tracking technologies used by companies — or, more broadly, companies' general gathering of information passively and using it for a variety of purposes. These cases are being filed under existing laws, including wiretap, pen register, video protection and biometric laws.

At the same time, these activities have been a focus of new U.S. state laws, and state regulators have issued guidance on how companies can engage in these practices without running afoul of these — or unfair and deceptive trade practice — laws, with provisions that specifically address digital tracking and profiling. We anticipate this trend continuing this year.

On the litigation front, cases this year have included Video Privacy Protection Act suits, like one filed against Viki Inc. — in Ade v. Viki Inc., in the U.S. District Court for the Northern District of California — where the court held that a plaintiff's consent to terms of use, which incorporate its privacy policy and cookie policy, is not sufficient consent under the VPPA.

In 2024 there were a spate of cases filed under California's Invasion of Privacy Act. Many allege that companies' use of tracking software constitutes an illegal pen register — i.e., a trap-and-trace device that captures dialing, routing, addressing or signaling information from a communication. To date, most have settled, but we expect companies to continue to receive cease-and-desist letters for these practices in 2025.

BIPA litigation continued in 2024 and may continue this year as companies continue to use facial recognition technologies, including for makeup try-on features, for instance.

On the legislative front, the U.S. state "comprehensive" privacy laws, including those passed in 2024 in Rhode Island, Minnesota, Maryland, Nebraska, Kentucky, New Hampshire and New Jersey, have also addressed passive tracking. They require, among other things, describing the company's practices and allowing people to opt out — for the most part — from having those tools used to serve targeted advertisements.

New York Attorney General Letitia James released guidance on these activities, finding that many companies' disclosures and choices were not working as described to consumers.[1] The U.K. Information Commissioner's Office was also focused on cookie disclosure and choice functionality in 2024.

To prepare for ongoing scrutiny in 2025, companies could take time to verify what passive tracking tools they are using, what information is being gathered, and if it is being shared with third parties. Also of importance is considering the extent to which vendors are assisting with the process, including advertising vendors or intermediaries. It would be prudent to ensure that the choices and disclosures being made are accurate, and to review and update them on a regular basis.

3. Combining and Sharing Data

The transfer of personal information between different entities, especially when there is an exchange of monetary or other consideration, was a focus in 2024. Companies whose business is to sell information, i.e., data brokers, already had registration requirements in Texas, Vermont and California. Oregon joined that list in 2024.

Additionally, in 2024, Texas Attorney General Ken Paxton indicated an intent to "rigorously enforce" his state's law. And in late 2024, California both conducted an investigate sweep and began the process of updating its law.[2]

The FTC also scrutinized data brokers, specifically where the exchange was of sensitive information, including geolocation information, or location information that might include someone being at a place of worship or health clinic. Often, according to the FTC, the individual did not know that their location information was being collected, and certainly not being used for advertising purposes. In some of the cases, including ones brought by the FTC against Mobilewalla, the information was included in audience segmentation data that was shared with third parties for advertising purposes.[3]

What can businesses do to prepare for 2025?

First, assess your data sharing practices, and keep in mind comprehensive laws that govern the sale of information — in particular, when the sale might be more than just a monetary exchange, which is true for laws in California, Connecticut, Colorado, Florida, Montana, Oregon, Texas Delaware, Maryland, Minnesota, Nebraska New Jersey, and New Hampshire, which go into effect this year.

And second, those who are data brokers, or who work with them, will want to keep a close watch on settlements that we anticipate will be coming out of the regulatory sweeps. These will likely signal regulatory expectations for use of personal data in the data broker environment.

4. Privacy Program Expectations

Companies' privacy compliance programs have long been a focus for regulators. They may look at a specific company's program during a privacy or data security investigation. They may also proactively provide guidance to the industry about program expectations.

We've also seen a rise in legislation dictating what elements should be included in a company's privacy program. Privacy compliance programs have also been a focus in litigation — especially litigation that arises after a data breach. We saw this trend increase in 2024, and expect it will pick up steam this year.

On the legislative front, for example, Oregon's comprehensive data privacy law, which took effect July 1, 2024, requires companies to evaluate and adjust security measures based on changing circumstances.[4]

On the enforcement side, the FTC has had a history of including privacy program management obligations in its consent decrees. An example is the $2.95 million settlement reached with security camera company Verkada in U.S. v. Verkada Inc., in the Northern District of California.[5] Among other things, the company agreed to implement a comprehensive security program monitored by third-party audits following a 2020 data breach.

Finally, there have been more developments in guidance from regulators and government agencies in terms of what is expected of companies' privacy programs. In a September 2024 update to the U.S. Department of Justice's sentencing guidelines for evaluating corporate compliance programs, the agency outlined its expectations of companies that find themselves in the agency's crosshairs.[6]

We expect that there will be ongoing scrutiny and regulation of corporate compliance programs. With this in mind, what steps can companies take?

Advice from the DOJ can come in handy here. This includes ensuring the program is designed to fit the company's specific needs. Elements to consider include policies, procedures, training and third-party oversight. It also includes ensuring that the program is properly funded, and the security team is empowered to act.

Finally, it includes ensuring that the program must actually function in practice. Change management tools in particular can help when thinking about getting leadership commitment and buy-in.

5. Managing Vendors

Vendor oversight remained a top concern for regulators, especially where vendors are handling personal data both in the U.S. and globally. We have seen action both in the U.S. and abroad.

Brazil unveiled specific contractual clauses for transferring data between businesses and to businesses' vendors.[7] In the U.S., seven more states — Rhode Island, Minnesota, Maryland, Nebraska, Kentucky, New Hampshire and New Jersey — passed laws with vendor management requirements. Minnesota, Maryland, Nebraska, New Hampshire and New Jersey's laws go into effect in 2025, and the rest in 2026.

These vendor-related obligations mirror those that exist under previously enacted "comprehensive" privacy laws and include having a contract in place with vendors, which describes the type of data, duration of processing, nature and purpose of processing, and guidelines for deletion or return of data.[8] The laws also require language that mandates confidentiality and cooperation with audits.[9] Vendors must also require subcontractors to be under contract and give proof of ongoing compliance.[10]

While most businesses have contractual provisions in place, best practices include carefully assessing vendors before onboarding them and providing them consumer information. Equally important and often forgotten is to continue to monitor vendors post-onboarding. This includes assessing vendors' technical measures as well as ensuring that consumer data is being used and stored as directed.

We can expect that regulators and consumers will litigate against vendors that are breached and the businesses who provided the data.

Liisa M. Thomas is the Chicago office managing partner and a co-leader of the privacy and cybersecurity practice at Sheppard Mullin Richter & Hampton LLP.

Kathryn Smith is an associate at the firm.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] New York State Attorney General, Website Privacy Controls, New York State Office of the Attorney General, available athttps://ag.ny.gov/resources/organizations/business-guidance/website-privacy-controls(last visited December 2, 2024).

[2] California Privacy Protection Agency, CPPA's Enforcement Division to Review Data Broker Compliance with the Delete Act, (Oct. 30, 2024), available at https://cppa.ca.gov/announcements/2024/20241030.html.

[3] In re Mobilewalla Inc., FTC File No. 202 3196 (2024).

[4] O.R.S. § 646A.622(2)(d)(A)(vi).

[5] United States v. Verkada Inc., No. 3:24-cv-06153 (N.D. Cal. 2024).

[6] U.S. Department of Justice – Criminal Division, Evaluation of Corporate Compliance Programs, (updated Sept. 2024), available at https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl.

[7] https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396.

[8] R.I. Gen. Laws § 6-48.1-7(2)(c) (effective Jan. 1, 2026); Minn. Stat. § 3250.04(c) (effective July 31, 2025); Md. Code Ann., Com. Law § 14-4608(A)(2) (effective Oct. 1, 2025); Neb. Rev. Stat. §87-1115(2) (operative Jan. 1, 2025); Ky. Rev. Stat. Ann. § 367.3619(2) (effective Jan. 1, 2026); N.H. Rev. Stat. Ann. §§ 507-H:7 (II) (effective Jan. 1, 2025); N.J. Stat. Ann. § 56:8-166.16(e) (effective Jan. 15, 2025).

[9] R.I. Gen. Laws § 6-48.1-7(2)(c) (effective Jan. 1, 2026); Minn. Stat. § 3250.04(c) (effective July 31, 2025); Md. Code Ann., Com. Law § 14-4608(A)(3) (effective Oct. 1, 2025); Neb. Rev. Stat. §87-1115(2)(f) (operative Jan. 1, 2025); Ky. Rev. Stat. Ann. § 367.3619(2) (effective Jan. 1, 2026); N.H. Rev. Stat. Ann. §§ 507-H:7 (II) (effective Jan. 1, 2025); N.J. Stat. Ann. § 56:8-166.16(e) (effective Jan. 15, 2025).

[10] R.I. Gen. Laws § 6-48.1-7(2)(c) (effective Jan. 1, 2026); Minn. Stat. § 3250.04(c)(2) (effective July 31, 2025); Md. Code Ann., Com. Law § 14-4608(A)(3) (effective Oct. 1, 2025); Neb. Rev. Stat. §87-1115(2)(f)(iii) (operative Jan. 1, 2025); Ky. Rev. Stat. Ann. § 367.3619(2) (effective Jan. 1, 2026); N.H. Rev. Stat. Ann. §§ 507-H:7 (II) (effective Jan. 1, 2025); N.J. Stat. Ann. § 56:8-166.16(e) (effective Jan. 15, 2025).