Hashed & Salted | A Privacy and Data Security Update
December 2024

End-of-Year Checklist: Are You Ready for the Next Wave of Privacy Laws?

2024 is quickly coming to a close and with it has brought a number of new state privacy laws. The U.S. now has 19 states with comprehensive privacy laws on the books and a handful of states with laws that specifically regulate health data or kids' data, among other specific categories of data, and next year this trend shows no signs of slowing down. While the change in administration and Federal Trade Commission (FTC) leadership will certainly bring changes to the privacy priorities at the federal level, the states appear poised to continue the U.S. privacy patchwork. At the top of 2025, comprehensive privacy laws in five additional states (Delaware, Iowa, Nebraska, New Hampshire and New Jersey) will come into effect. We expect to see several states pass comprehensive privacy laws in 2025, in addition to laws focusing on health data, and kids' and teen data, as well as broader data governance laws that intersect with efforts to regulate artificial intelligence. 2025 will bring new rulemaking in California and New York, as well as an expected increase in enforcement. Outside of California, Texas is emerging as a key contender in this space, with several investigations announced in the last quarter of 2024. Now is a great time to check to make sure you are setting yourself up for a scalable privacy program that is designed to adapt to this changing landscape.

To help you stay updated on the complex landscape of privacy laws in the U.S., we've launched Loeb & Loeb's Privacy Law Resource Center app, your ultimate tool for understanding and managing privacy regulations. The app offers a comprehensive set of features, including a guide to all the comprehensive U.S. state privacy laws; an Interactive Statute Comparison Tool, allowing users to compare different sections of state privacy laws; and a U.S. State Breach Notification Chart detailing breach notification requirements. The app also gives users access to privacy law resources and webinars, as well as customizable notifications and exclusive registered content for Loeb clients:

Scan the QR code to download the app or visit privacy.loebapps.com to access the web app.

Visit qr.loeb.com/privacylaw to request a client access code, or reach out to your Loeb contact directly.

New State Laws: What Do You Need To Know?

While there are many similarities in the growing body of state laws, companies should consider whether the new laws will require updates to privacy notices, the consumer rights process, data governance policies, security controls, and their approach to sensitive and kids' data.

Privacy Notice Updates

Most states tie their privacy disclosures to the data collection that has taken place in the last 12 months.

Attorney Advertising

Privacy notices should generally be reviewed at least once a year, and the end of the year is a good time to check in to confirm that all your notices reflect the reality of your current and planned processing activities. If you have been listing all the states that your privacy notice applies to or maintaining separate sections in your privacy notice for each state, now is a good time to revisit whether it continues to make sense to take that approach in light of the number of states with active privacy laws. While the requirements for privacy notices are largely the same across the new states, New Jersey requires the notice to be presented in a manner that is similar to California's notice-at-collection requirements.

Consumer Rights

In addition to privacy notice updates, the end of the year is a great time to confirm that your consumer rights process is working and to check any channels of consumer communications (including privacy and other email inboxes and customer service lines) to make sure messages haven't been missed. Check social media and other platforms for any complaints about your company's privacy practices to make sure you're not missing the chance to get ahead of any consumer complaints.

Fortunately, all the states with privacy laws coming into effect before Feb. 2, 2025, have the same core of consumer rights—to confirm processing, access personal information, correct inaccurate information, delete personal information and obtain a portable copy (when/if feasible). Likewise, most states provide a right to opt out of sale, targeted advertising and profiling with legal or other significant effects. Most of the new states will also require companies to provide a right to appeal the denial of an opt-out. There is a rolling timeline under the new slate of state laws for companies to respond to universal opt-out mechanisms:

- Jan. 1, 2025 – Montana, Nebraska, New Hampshire
- July 15, 2025 – New Jersey
- Jan. 1, 2026 – Delaware, Oregon

Oregon and New Jersey have added the right to receive a list of the specific third parties to which the business has disclosed information about either that consumer or all consumers. California's current rulemaking package on automated decision-making technology (ADMT) includes the right to access and opt out of or appeal ADMT decisions, but those obligations could shift before those rules become final.

Data Governance

As privacy regulation and enforcement move into their next phase of maturity, companies will need to adjust their privacy programs to keep up. While the consumer-facing elements of a privacy notice, consumer rights and opt-out mechanisms are often priority items, companies should not forget that all state privacy laws also require robust internal data governance programs that address requirements to practice data minimization and purpose limitation, manage and audit/oversee vendors, identify and address any high-risk uses of data, and perform impact assessments where necessary.

Audit/Vendor Management

Vendor management has been flagged as a priority across a number of jurisdictions. It is no longer sufficient to rely on contractual protections. Companies are expected to assess the data protection practices of their partners at the beginning of the relationship, as well as throughout the life cycle of the vendor relationship.

Data Protection/Risk Assessments

Most states will require companies to conduct data protection assessments for high-risk activities, which include the sale of data, targeted advertising, and the use of sensitive data and profiling that creates a risk for things like discrimination, unfairness, and financial or physical injury.

Security Controls

Mst of the state laws contain requirements for companies to implement "reasonable" security controls. These include technical and organizational measures to protect against unauthorized access, use, disclosure, alteration or destruction. What is reasonable, however, will depend on the volume and nature of the data that you store or maintain on your systems. Companies may look to NIST, ISO 270001 or CIS controls as benchmarks to measure their security controls. In Oregon, security measures must comply with ORS 646A.622. Finally, California's rulemaking on cybersecurity audits may require companies that engage in activities that pose a significant risk to consumers (which include processing sensitive personal information, and deriving significant revenue from the sale or sharing of personal information) to comply with a series of security controls that include implementing a zero trust architecture and implementing data retention schedules.

Consent for Sensitive Personal Information

While states like Iowa have followed California's lead in allowing businesses to collect sensitive personal information until someone opts out, several states have taken the path outlined by Virginia and Connecticut, requiring opt-in consent. Nebraska, New Hampshire and New Jersey will all require opt-in consent starting in January 2025, while Oregon's, Texas' and Montana's requirements to obtain opt-in consent went into effect earlier this year. Companies in Oregon must specify the purposes for which they collect and process sensitive personal information and obtain fresh consent for incompatible purposes. If a company is selling the sensitive personal information of residents of Texas, they should have the following notice on their website: "NOTICE: We may sell your sensitive personal information."

Sensitive personal information typically includes data revealing racial or ethnic origin, religious beliefs, health conditions, sexual orientation, and genetic or biometric data.

Special Rules for Kids' Data

Recent state laws have reflected the growing concern about the use of personal information collected from children. While most states defer to the Children's Online Privacy Protection Act (COPPA) for data collected from kids under age 13, they have added more requirements for minors under age 17. Oregon, New Jersey and New Hampshire all require consent to process personal information for targeted advertising, profiling and selling involving minors known to be 13 to 17 years of age. Whether a company "knows" an individual is 13 to 17 varies by state, with some states including "willful disregard" in their knowledge standard.

Connecticut's SB3, which amended the Connecticut Consumer Data Privacy Act (CDPA), creates new obligations for online services, products and features directed to minors under 18. Companies must now use reasonable care to avoid heightened risk of harm to minors under 18. Consent is required prior to using personal data for targeted advertising or profiling, the sale of personal data, and the use of a design feature to significantly increase, sustain or extend any minor's use of the online service, product or feature. For processing of precise geolocation information, companies must both obtain consent and provide a signal to the minor that precise geolocation data is being collected for the entire duration of the collection.

Companies will need to conduct a CDPA-compliant Data Protection Impact Assessment (DPIA) to assess any heightened risk of harm to minors that is a reasonably foreseeable result of offering the online service, product or feature to minors; implement a plan to mitigate or eliminate any risks identified in their DPIAs; and maintain these DPIAs for the life of the online service, product or feature, plus an additional three years.

Key Takeaways: Your End-of-Year Checklist

- Review and update privacy notices.
- Update mechanisms for consumer rights: Expand as needed to address new requirements, new states, or new requirements for appeals.
- Strengthen data governance practices: Determine whether/when DPIAs should be performed; implement data minimization principles through product reviews designed to limit data collection to what is needed for the product (which may include data needed to deliver ads for ad-supported products); review contracts with service providers and third parties; and consider whether your diligence and audit programs need to be updated to address any audit or oversight obligations.
- Evaluate and strengthen security measures to protect personal data.
- Establish consent procedures for sensitive information, or confirm that your company is not collecting sensitive personal information.
- Review and update policies for children's data (and if you take the position that your platform is not directed to or does not have a child audience, document that analysis).

Related Professional

Jessica B. Lee . . . . . jblee@loeb.com