2024 Privacy Legislative Roundup

Lizzi Esparza
eesparza@mwlaw.com
(479) 464.5660

12/11/2024

2024 was a banner year for state privacy legislation. This year saw seven new states pass comprehensive consumer privacy laws, joining the ranks of 12 other states that have previously passed similar laws. While other state laws followed a general pattern with marginal variances in definitions and applicability thresholds, these new seven laws contain additional requirements and nuance that separate them from the pack.

Comprehensive State Consumer Privacy Laws

Each state privacy law governs an entity's processing of personal data, defined as any information that is "linked or reasonably linkable to an identified or identifiable" natural person, but not including de-identified or publicly available data.

Each of the following states require businesses and organizations subject to their respective law's applicability to provide the following rights to residents: (1) right to access data, (2) right to correct, (3) right to delete, (4) right to opt out of targeted advertising / cross-contextual behavioral advertising, (5) right to opt out of the sale of personal data, (6) right to data portability.

Except where indicated below, each state law requires a business to provide a consumer privacy notice disclosing privacy practices, including the rights enumerated above and how to exercise them. Additionally, businesses must disclose the categories of third parties with which a business shares personal data. Further, entities must obtain consent before processing sensitive personal information (defined differently in each state, but generally including data revealing a person's race, ethnic origin, sexual orientation, religious beliefs, precise geolocation, etc.).

States remain divided on the issue of requiring entities to recognize universal opt-out mechanisms (UOOM), referring to a range of tools that send a standardized signal to websites that a user has opted out of collection of their personal information. Nebraska, Minnesota, New Jersey, and Maryland each require entities to recognize the use of UOOM, whereas New Hampshire, Kentucky, and Rhode Island do not.

Following the national trend, each of the seven new state laws contain exemptions for employee data, HIPAA- and GLBA-regulated entities, and business-to-business transfers of data. All but Minnesota and New Jersey contain an exemption for nonprofit organizations.

In order of effective date, differences (where applicable) between the seven state laws are highlighted below.

- **New Hampshire**
- New Hampshire Privacy Act, N.H. SB 255.
- Effective January 1, 2025.
- **New Jersey**

- New Jersey Data Protection Act, N.J. SB 332.
- Effective January 15, 2025.
- No nonprofit exemption.
- Includes status as transgender or nonbinary, genetic or biometric data, and finance-related information in its definition of "sensitive personal information."
- Grants rulemaking authority to its Division of Consumer Affairs.
- **Minnesota**
- Minnesota Consumer Data Privacy Act, Minn. HF 4757.
- Effective July 31, 2025.
- Grants residents who have been subject to automated profiling (i.e., algorithmic decision-making) "the right to question the result of the profiling, to be informed of the reason for profiling, to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions the consumer might have taken to secure a different decision in the future."
- No nonprofit exemption.
- However, small businesses (as defined by the US Small Business Administration) are exempt from the law.
- **Nebraska**
- Nebraska Data Privacy Act, Neb. HF 4757.
- Effective July 31, 2025.
- Unlike the majority of states, Nebraska's law does not contain a threshold for processing resident data. Said otherwise, if an organization processes data of any Nebraska resident, Nebraska's law applies to that processing. However, like Minnesota, Nebraska also contains a small business exemption.
- **Maryland**
- Maryland Online Data Privacy Act, Md. SB 541.
- Effective October 1, 2025.
- Creates a heightened standard for data-minimization, requiring entities to limit collection of personal data to what is "reasonably necessary and proportionate to provide or maintain a specific product or service requested" by the individual. Collection and processing of sensitive data must be "strictly necessary to provide or maintain a requested product or service." This first-in-class standard may create challenges for affected entities.
- Includes national origin, status as transgender or nonbinary, and consumer health data in its definition of "sensitive personal information."
- **Kentucky**
- Kentucky Consumer Data Privacy Act, Ky. HB 15.
- Effective January 1, 2026.
- **Rhode Island**
- Rhode Island Data Transparency and Privacy Protection Act, R.I. HB 7787.
- Effective January 1, 2026.
- Requires disclosure of specific list of third parties (not just categories of third parties).
- No requirement for data minimization or purpose limitation.

Other Legislative Trends

- **Sensitive data.** Colorado and California each amended their respective comprehensive consumer privacy laws to include "neural data" as a protected piece of sensitive personal data. *See* Colo. HB 24-058 & Cal. SB No. 1223. In Colorado, "neural data" refers to "information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a device." In California, the term means "information that is generated by measuring the activity of a consumer's central or peripheral nervous system and that is not inferred from nonneural information."

- **Children's privacy.** Virginia added new protections for children's data to the Virginia Consumer Data Protection Act.
- **Biometric privacy.**
- Colorado amended the Colorado Privacy Act to add provisions related to biometric privacy, including prohibiting collection without first satisfying certain disclosure and consent requirements, requiring a written policy pertaining to retention of biometric identifiers, and restricting an employer's permissible reasons for collecting biometric identifiers. *See* Colo. HB24-1130.
- Illinois amended its Biometric Information Privacy Act to clarify that only one cause of action is created where an entity processes either the same biometric identifier multiple times, or multiple biometric identifiers of the same person, reversing a prior Illinois Supreme Court holding to the contrary. *See* Ill. Pub. Act 103-0769.
- **Artificial intelligence.** Several state legislatures introduced bills aimed at regulating artificial intelligence, but only Utah and Colorado passed legislation.
- Utah's Artificial Intelligence Policy Act establishes liability for use of AI that violates consumer protection laws if the use is not appropriately disclosed, and vests regulatory authority in the newly created Office of Artificial Intelligence Policy. *See* Utah S.B. 149.
- Colorado became the first state to pass a bill aimed at mitigating algorithmic discrimination in "high-risk artificial intelligence systems" (defined as an AI system that, when deployed, makes, or is a substantial factor in making, a decision having an impact on education enrollment or opportunity, employment, financial or lending services, essential government services, healthcare services, housing, insurance, or legal service). *See* Colo. SB24-205.

In the absence of a federal data privacy law, the patchwork of state data protection laws increases in complexity with each passing year. With almost half of all states having passed consumer privacy laws, and others regulating the use of new and developing technologies, businesses and organizations should keep their privacy programs top of mind. Even businesses not located in states with a comprehensive consumer privacy law may be subject to their requirements if they do business in a particular state.

Lizzi Esparza focuses her practice on information privacy, security and data rights law. She is a Certified Information Privacy Professional/United States (CIPP/US) and a Certified Information Privacy Professional/Europe (CIPP/E).