Published on *The National Law Review* https://natlawreview.com

Consumer Privacy Update: What Organizations Need to Know About Impending State Privacy Laws Going into Effect in 2024 and 2025

Article By:

Alaap B. Shah

Audrey Davis

Amy Cooperstein

Over the past several years, the number of states with comprehensive consumer data privacy laws has increased exponentially from just a handful—California, Colorado, Virginia, Connecticut, and Utah—to up to twenty by some counts.

Many of these state laws will go into effect starting Q4 of 2024 through 2025. We have previously written in more detail on New Jersey's comprehensive data privacy law, which goes into effect January 15, 2025, and Tennessee's comprehensive data privacy law, which goes into effect July 1, 2025. Some laws have already gone into effect, like Texas's Data Privacy and Security Act, and Oregon's Consumer Privacy Act, both of which became effective July of 2024. Now is a good time to take stock of the current landscape as the next batch of state privacy laws go into effect.

Over the next year, the following laws will become effective:

1. Montana Consumer Data Privacy Act (effective Oct. 1, 2024)
2. Delaware Personal Data Privacy Act (effective Jan. 1, 2025)
3. Iowa Consumer Data Protection Act (effective Jan. 1, 2025)
4. Nebraska Data Privacy Act (effective Jan. 1, 2025)
5. New Hampshire Privacy Act (effective Jan. 1, 2025)
6. New Jersey Data Privacy Act (effective Jan. 15, 2025)
7. Tennessee Information Protection Act (effective July 1, 2025)
8. Minnesota Consumer Data Privacy Act (effective July 31, 2025)
9. Maryland Online Data Privacy Act (effective Oct. 1, 2025)

These nine state privacy laws contain many similarities, broadly conforming to the Virginia Consumer Data Protection Act we discussed here. All nine laws listed above contain the following familiar requirements:

(1) disclosing data handling practices to consumers,

(2) including certain contractual terms in data processing agreements,

(3) performing risk assessments (with the exception of Iowa); and

(4) affording resident consumers with certain rights, such as the right to access or know the personal data processed by a business, the right to correct any inaccurate personal data, the right to request deletion of personal data, the right to opt out of targeted advertising or the sale of personal data, and the right to opt out of the processing sensitive information.

The laws contain more than a few noteworthy differences. Each of the laws differs in terms of the scope of their application. The applicability thresholds vary based on: (1) the number of state residents whose personal data the company (or "controller") controls or processes, or (2) the proportion of revenue a controller derives from the sale of personal data. Maryland, Delaware, and New Hampshire each have a 35,000 consumer processing threshold. Nebraska, similar to the recently passed data privacy law in Texas, applies to controllers that that do not qualify as small business and process personal data or engage in personal data sales. It is also important to note that Iowa adopted a comparatively narrower definition of what constitutes as sale of personal data to only transactions involving monetary consideration. All states require that the company conduct business in the state.

With respect to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Iowa's, Montana's, Nebraska's, New Hampshire's, and Tennessee's laws exempt HIPAA-regulated entities altogether; while Delaware's, Maryland's, Minnesota's, and New Jersey's laws exempt only protected health information ("PHI") under HIPAA. As a result, HIPAA-regulated entities will have the added burden of assessing whether data is covered by HIPAA or an applicable state privacy law.

With respect to the Gramm-Leach-Bliley Act ("GLBA"), eight of these nine comprehensive privacy laws contain an entity-level exemption for GBLA-covered financial institutions. By contrast, Minnesota's law exempts only data regulated by GLBA. Minnesota joins California and Oregon as the three state consumer privacy laws with information-level GLBA exemptions.

Not least of all, Maryland's law stands apart from the other data privacy laws due to a number of unique obligations, including:

- A prohibition on the collection, processing, and sharing of a consumer's sensitive data except when doing so is "strictly necessary to provide or maintain a specific product or service requested by the consumer."
- A broad prohibition on the sale of sensitive data for monetary or other valuable consideration unless such sale is necessary to provide or maintain a specific product or service requested by a consumer.
- Special provisions applicable to "Consumer Health Data" processed by entities not regulated by HIPAA. Note that "Consumer Health Data" laws also exist in Nevada, Washington, and Connecticut as we previously discussed here.
- A prohibition on selling or processing minors' data for targeted advertising if the controller knows or should have known that the consumer is under 18 years of age.

While states continue to enact comprehensive data privacy laws, there remains the possibility of a federal privacy law to bring in a national standard. The American Privacy Rights Act ("APRA")

recently went through several iterations in the House Committee on Energy and Commerce this year, and it reflects many of the elements of these state laws, including transparency requirements and consumer rights. A key sticking point, however, continues to be the broad private right of action included in the proposed APRA but absent from all state privacy laws. Only California's law, which we discussed here, has a private right of action, although it is narrowly circumscribed to data breaches. Considering the November 2024 election cycle, it is likely that federal efforts to create a comprehensive privacy law will stall until the election cycle is over and the composition of the White House and Congress is known.

National Law Review, Volume XIV, Number 257