Now & Next
Privacy & Technology Alert

April 21, 2026

Practical guidance for organizations navigating US State Privacy law requirements

By Jacqueline Cooney, Jenny Holmes, and Hannah Edmonds

US state privacy laws are turning privacy policies into compliance documents—requiring more specific disclosures, new AI-related statements, and expanded consumer rights.

What's the impact?

- Privacy policies that only describe data practices at a high level may fall short, as more states require prescriptive disclosures, including identifying specific third parties in certain contexts.
- Connecticut's July 1, 2026, amendments raise the bar by requiring organizations to affirmatively disclose whether personal information is collected, used, or sold for large language model training—driving immediate need for data mapping and vendor diligence.
- Expanded consumer rights tied to profiling and automated decision-making mean organizations must not only update policy language, but also operationalize workflows to intake, investigate, and respond to more complex requests.

Once a simple matter of publishing clear information about how companies collect and use personal information, website privacy policies are increasingly required to meet specific regulatory requirements imposed by nearly two dozen different laws across the US.

Simply having a privacy policy posted on a company website is no longer enough—companies must now disclose certain uses of data in prescriptive ways, as outlined by the various laws. And, because a company's website privacy policy is posted publicly for all to see (including regulators), companies that fail to update their policies risk enforcement actions and reputational harm.

Reviewing, understanding, and implementing all the different requirements regularly to keep up with the ever-changing laws can seem like an overwhelming task. We provide a roadmap here to address key requirements and reduce risk.

Disclose which third parties receive personal information

THE EVOLVING REQUIREMENT

Most state privacy laws require organizations to disclose only the categories of third parties to whom they disclose personal information (e.g., "advertising partners" or "analytics providers"). A growing number of states, however, now require disclosure of *specific, named* third parties, giving consumers significantly greater transparency.

KEY STATE LAWS TO MONITOR

- **Minnesota Consumer Data Privacy Act (MCDPA), Delaware Personal Data Privacy Act (DPDPA)**, and **Oregon Consumer Privacy Act (OCPA):** Consumers have the right to obtain a list of the specific third parties to which an organization has disclosed their personal information.
- **Connecticut Data Privacy Act (CTDPA)** (amendments effective July 1, 2026): Consumers will have the right to obtain a list of specific third parties to whom an organization has *sold* their personal information.
- **Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA)** (effective January 1, 2026): Organizations must identify all third parties to whom consumers' personal information has been *sold or may be sold*, posted in a conspicuous location on the organization's website or online service platform where customer agreements or similar notices are customarily posted (which could include a privacy policy).

RECOMMENDED ACTION ITEMS

- **Update the consumer rights section** of your privacy policy to include the right to obtain a list

of specific third parties, where the MCDPA, DPDPA, OCPA, or CTDPA (as amended) apply to your organization.

- **Build and maintain an internal list** of all third parties to whom personal information is disclosed, with a notation of which third parties receive personal information through a sale. This list is essential for responding to consumer rights requests in a timely and accurate manner.
- **For RIDTPPA compliance**, maintain a list of third parties to whom personal information is *sold or may be sold*, and update your privacy policy to direct consumers to the location where that list is available. For example, if the list is housed in a cookie policy or a cookie/privacy preferences center (because you "sell" personal information via third-party online tracking), the privacy policy should include a cross-reference directing consumers to that location.

Disclosing use of personal information for large language model training in Connecticut

THE EVOLVING REQUIREMENT

Connecticut will be the first state to require organizations to disclose in their privacy policies whether they collect, use, or sell personal information for the purpose of training large language models (LLMs). This requirement, part of the CTDPA amendments taking effect July 1, 2026, applies regardless of whether the organization engages in such activity. In other words, organizations must affirmatively state that they do or do not use personal information for LLM training. This requirement signals broader regulatory interest in AI-related data practices.

RECOMMENDED ACTION ITEMS

- **Conduct an internal audit** of your data processing activities to determine whether personal information is collected, used, or sold to train LLMs, whether directly or indirectly, through vendors and service providers.
- **Interpret "LLM" broadly**. The CTDPA amendments do not define the term. Organizations should err on the conservative side when assessing whether any AI systems they use or support could qualify as an LLM.
- **Add a clear disclosure statement** to your privacy policy indicating whether you do or do not collect, use, or sell personal information for LLM training purposes.
- **Review vendor and service provider contracts** to identify any downstream use of personal information for LLM training that may need to be disclosed.

Addressing consumer rights related to profiling

THE EVOLVING REQUIREMENT

Several states are expanding consumer rights around the use of personal information for profiling, particularly when profiling leads to automated decision-making that produces legal or similarly significant effects on consumers. These rights go beyond a simple opt-out and give consumers tools to understand and challenge profiling decisions.

KEY STATES TO MONITOR

Minnesota – MCDPA: Where profiling produces legal or similarly significant effects, consumers have the right to the following:

- Question the result of such profiling.
- Be informed of what actions the consumer may have taken to secure a different decision, and what actions the consumer may take in the future.
- Review the personal information used in the profiling.
- If a decision is based on inaccurate personal information, have it corrected and the profiling decision reevaluated based on the corrected information.

Connecticut – CTDPA (amendments effective July 1, 2026): Where profiling results in an automated decision producing legal or similarly significant effects, consumers will have the right to take the following actions:

- Question the result of such profiling.
- Be informed of the reason the profiling resulted in the decision.
- Review the personal information processed for purposes of such profiling.
- If the profiling decision concerned housing, correct any inaccurate personal information and have the profiling decision reevaluated.

RECOMMENDED ACTION ITEMS

- **Update the consumer rights section** of your privacy policy to include the profiling-related rights described above, where the MCDPA or CTDPA (as amended) apply to your organization.
- **Establish internal processes and procedures** to receive, evaluate, and respond to consumer requests related to profiling in a timely and accurate manner.
- **Coordinate** with business teams that use automated decision-making tools to ensure they can identify when profiling produces legal or similarly significant effects and can support consumer rights requests.

How Nixon Peabody can help

Nixon Peabody's cybersecurity and privacy attorneys regularly partner with clients on a wide array of compliance initiatives, including determining privacy law applicability, updating privacy policies, and building the internal processes needed to operationalize compliance. Our team can also recommend safeguards and other measures to ensure the security of your data and, in turn, your reputation. If you have questions concerning state privacy law applicability or privacy policy disclosure requirements and best practices, please do not hesitate to contact a member of our practice.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Jacqueline W. Cooney
617.345.6180
jcooney@nixonpeabody.com

Jenny L. Holmes
585.263.1494
jholmes@nixonpeabody.com

Hannah Edmonds
202.585.8370
hedmonds@nixonpeabody.com