

The Evolving State Privacy Landscape: Major Updates to Consumer Privacy Laws in Montana and Connecticut

October 15, 2025

Montana and Connecticut have amended their consumer privacy laws to make a number of significant changes, including introducing new protections for minors, lowering applicability thresholds, imposing further requirements on privacy notices and eliminating or narrowing certain exemptions. The amendments to the Montana Consumer Data Privacy Act (MTCDPA) took effect on October 1, 2025, while (most of) the amendments to the Connecticut Data Privacy Act (CTDPA) will take effect on July 1, 2026.

The amendments to the MTCDPA, like the recent amendments expanding Montana's Genetic Information Privacy Act to cover neural data, passed the Montana Legislature with an overwhelming majority. Meanwhile, the latest CTDPA amendments continue Connecticut's pattern of amending its consumer privacy law. These developments signal that consumer privacy regimes continue to evolve and remain a significant – and often bipartisan – priority at the state level. They are also part of a larger trend where states, facing a murky legal landscape and continued lack of movement on privacy at a federal level, borrow from one another's approaches to addressing emerging privacy-related concerns – for example, related to the collection and use of minors' data.

Below, we explain key changes to the MTCDPA and CTDPA, as well as what companies should do to assess their impact and address potential compliance gaps.

Montana

Increased protections for minors

- **Duty of care:** The amended MTCDPA requires any company that offers an online service, product or feature to a consumer the controller actually knows, or willfully disregards, is a minor (defined as under 18) to use “reasonable care” to avoid a “heightened risk of harm to minors.” The updates also impose additional consent requirements and data usage restrictions for minors. Additionally, if there is a heightened risk of harm to minors, the company must also conduct a data protection assessment. Together, the duty of care and related obligations could impact the design of companies' products and services, or at least the versions of those products and services used by minors.
- **No minimum thresholds:** Notably, these new obligations related to minors apply to **all** companies that conduct business in Montana or deliver commercial products or services that are intentionally targeted to Montana residents – not just companies that meet the minimum applicability thresholds that apply to most of the MTCDPA's other obligations (see below).
- **Age verification not required:** The amended MTCDPA also contains a disclaimer that these new requirements should not be construed to require age verification. This was likely a gesture at the history of age verification requirements being struck down on First Amendment grounds. But after the US Supreme Court's recent decision upholding a Texas age verification law in *Free Speech Coalition, Inc. v. Paxton*, states may not shy away from age verification requirements in the future.

Additional rights/opt outs and privacy notice requirements

- **Additional obligations for data sales and targeted advertising:** If a controller sells personal data to third parties or processes personal data for targeted advertising, it must disclose such activities in its privacy notice and give the consumer the ability to opt out.
- **Additional privacy policy requirements:** The amended MTCDPA includes other prescriptive requirements for privacy notices and related disclosures, such as requiring companies to provide a privacy notice in each language in which the company provides products and services, and in a manner reasonably accessible and usable to individuals with disabilities.
- **Treatment of sensitive data in consumer rights requests:** In response to a consumer's request for their personal data under the MTCDPA's access right, a controller who has collected certain sensitive types of data (e.g., Social Security

numbers, financial account numbers, account passwords) must not disclose the sensitive data itself. Instead, the controller must inform the consumer with sufficient particularity that the controller has collected such sensitive data. This new requirement appears designed to prevent an individual's sensitive data from being inadvertently exposed through fulfillment of a rights request – for example, if a company uses an insecure method to share a copy of the requestor's data.

Expanded applicability

- **Lower thresholds:** After the amendments, the MTCDDPA applies to entities that control/process the personal data of at least 25,000 (down from 50,000) Montana residents, or control/process the personal data of at least 15,000 (down from 25,000) Montana residents and generate more than 25% of their gross revenue from the sale of personal data. The new 25,000-resident threshold is, in absolute terms, the lowest among states whose consumer privacy laws include such numerical thresholds – though it is less of an outlier relative to Montana's (modest) population.
- **Changes to entity-level exemptions:** The amendments eliminate the entity-level exemption for financial institutions and affiliates governed by the Gramm-Leach-Bliley Act (GLBA) but keep the GLBA data-level exemption. They also create new entity-level exemptions for "state or federally chartered banks, credit unions, affiliates or subsidiaries that are principally engaged in financial activities," but these will likely not cover all entities that were covered by the previous GLBA entity-level exemption.
- **Narrower nonprofit exemption:** The amendments substantially narrow the MTCDDPA's nonprofit exemption to apply only to nonprofits that are "established to detect and prevent fraudulent acts in connection with insurance."

Enhanced enforcement authority and penalties

- **Increased investigative powers and no required cure period:** The amendments broaden the MTCDDPA's enforcement provisions and increase the Montana attorney general's investigatory powers. Notably, the attorney general can now issue civil investigative demands and is no longer required to offer controllers an opportunity to cure before bringing an enforcement action.
- **New civil penalties:** The amendments also add a new civil penalty provision to the MTCDDPA under which the attorney general can seek up to \$7,500 per violation. The per-violation nature of the penalties means that they could easily reach significant dollar amounts if a company's violative practices extend across a large number of Montana residents.

Connecticut

Increased protections for minors

- **Limitations on collection/processing of minors' personal data:** Under the amended CTDDPA, a controller cannot process the personal data of anyone it actually knows or willfully disregards is a minor (defined as under 18) unless the processing is reasonably necessary for the company's service. And even if that standard is met, the CTDDPA requires that minors' data only be processed for the purpose disclosed at the time of collection and only for as long as is reasonably necessary. Controllers also cannot collect precise geolocation data from minors unless the data is strictly necessary for the service and the company indicates it is doing so at the time of collection.
- **Bans on targeted advertising and personal data sales:** The amended CTDDPA prohibits controllers from processing minors' personal data for targeted advertising or selling minors' personal data. Importantly, these are outright bans that cannot be overcome by, for example, obtaining (parental) consent to process minors' data in these ways. As such, they could significantly impact the data handling practices and business models of companies whose services are targeted at or used by minors.

Additional rights/opt outs and privacy notice requirements

- **Rights related to derived/inferred data and profiling:** The amendments expand the CTDDPA's access right to include inferences about the individual derived from personal data and whether the personal data is being used for profiling to make a decision that produces legal or similarly significant effects about the consumer. The amendments also grant consumers the right to contest profiling decisions.
- **Disclosure of large language model training:** Companies must disclose whether they collect, use or sell personal data for the purpose of training large language models.

- **Treatment of sensitive data in rights requests:** Paralleling the amended MTCDDPA (see above), companies responding to a consumer request cannot disclose sensitive data itself and must instead inform the consumer with sufficient particularity that the controller has collected such sensitive data.

Expanded applicability

- **Lowered numerical thresholds:** The CTDDPA's main numerical threshold is being lowered to apply to entities that control/process the personal data of at least 35,000 Connecticut residents (down significantly from 100,000).
- **Other new thresholds:** The amendments also add two further threshold activities that are **not** subject to any numerical minimums:
 1. Controlling or processing Connecticut residents' sensitive data (excluding personal data controlled or processed solely for the purpose of completing a payment transaction).
 2. Offering Connecticut residents' personal data for sale in trade or commerce.

The latter will replace a similar, but less stringent, threshold under which the CTDDPA applies to entities that control/process the personal information of 25,000+ Connecticut residents **and** derive at least 25% of their revenue from personal data sales. Importantly, because “sensitive data” (see below) and “sales” are both defined broadly under the CTDDPA, these two new thresholds could result in many companies becoming newly subject to the law.

- **Expanded definition of “sensitive data”:** The amended CTDDPA expands the definition of sensitive data to include disability or treatment; status as nonbinary or transgender; neural data (defined as “any information that is generated by measuring the activity of an individual's central nervous system”); a consumer's financial account number, financial account login information, or credit card or debit card number, and government-issued identification numbers (e.g., Social Security numbers).
- **Changes to entity-level exemptions:** As in Montana, the amendments to the CTDDPA eliminate the entity-level exemption for financial institutions and affiliates governed by the GLBA but keep the GLBA data-level exemption. The amendments also create narrower entity-level exemptions for certain financial institutions (e.g., insurers, banks, credit unions).

Impact assessment obligations

- **Impact assessment for profiling:** The amended CTDDPA requires controllers to conduct an impact assessment if they engage in profiling for the purpose of making a decision that produces a legal or similarly significant effect concerning a consumer. The law also includes prescriptive requirements for what the impact assessment must cover – including, among other things, the intended use cases and deployment of the profiling and its intended benefits; an analysis of any known or reasonably foreseeable heightened risk of harm to a consumer; mitigation steps; a description of the inputs and outputs involved; and whether the controller discloses the use of profiling to consumers.
- **Mitigation requirements:** The amendments also require that if a controller conducts an impact assessment and determines that there is a heightened risk of harm to minors, the controller must establish and implement a plan to mitigate or eliminate such risk.

What companies should do

Companies that do business in Montana and/or Connecticut should take steps to evaluate new obligations and address potential compliance gaps under the states' updated privacy laws, for instance by:

- Assessing whether the company could become newly subject to the MTCDDPA and/or CTDDPA due to the changes in the laws' thresholds and exemptions.
- Evaluating whether the company is engaging in activities that could be impacted by the laws' new protections for minors, such as Montana's duty of care or Connecticut's ban on targeted advertising using minors' personal data.
- Analyzing what changes to the company's products and services or data handling activities may be needed to comply with the laws' new requirements related to minors.
- Assessing whether any of the company's data processing activities could constitute profiling that is subject to new impact assessment obligations and rights.

- To the extent not already done to comply with similar requirements under other US state consumer privacy laws:
 1. Updating the company's privacy policy to address additional prescriptive requirements, such as offering the privacy policy in additional languages in which the company offers products and services and in a disability-accessible format.
 2. Reviewing and updating policies and procedures for handling data subject requests to address additional opt-outs, rights and data subject handling request requirements.

Kara Kelawan, a cyber/data/privacy summer associate, also contributed to the preparation of this client alert.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our [legal notices](#).

Key Contacts

Kristen Mathews New York	kmathews@cooley.com
Christopher Suhler Colorado	csuhler@cooley.com +1 720 566 4376

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.