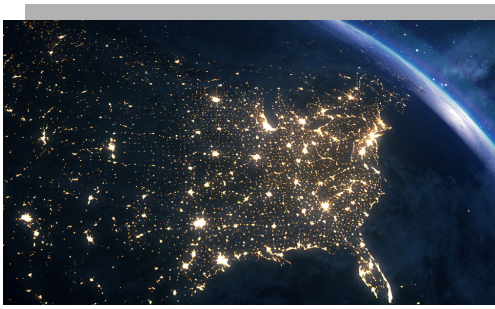
What You Need To Know



- 19 state comprehensive privacy laws have been enacted to date, and three (Oregon, Texas, and Montana) will take effect in 2024, which will introduce some new requirements and application thresholds.
- Washington and Nevada health data laws took effect March 31, 2024, imposing consent and other requirements for consumer health data, which is broadly defined.
- California and Connecticut took assertive steps to enforce their respective privacy laws, with investigative sweeps, and enforcement actions, advisories, and reviews.
- California rulemaking regarding automated decision-making technology continues, with sweeping regulations in the offing.

The State Comprehensive Privacy Mill Keeps Churning

Six states – Nebraska, New Hampshire, New Jersey, Kentucky, Maryland, and Minnesota – have enacted comprehensive privacy laws so far this year, bringing the total to 19. Three of those 19, Oregon, Texas, and Montana, will take effect in 2024, bringing the number of active comprehensive privacy laws to eight.

Thankfully for most businesses, these new laws borrow several elements from previously enacted comprehensive privacy laws, which will help companies navigate the ever-increasing patchwork of state privacy laws. However, the new laws do introduce some new elements that companies will need to incorporate into their privacy compliance strategies.

- **Oregon:** The Oregon Consumer Privacy Act, which takes effect July 1, 2024, will introduce some new "sensitive data" categories. Specifically, personal data revealing a consumer's national origin, status as a victim of crime, or status as transgender or non-binary will constitute "Sensitive Data," requiring consumer consent for processing. Oregon also provides consumers with the right to obtain from a controller a list of specific third parties to which the controller has disclosed either (at the controller's option): that specific consumer's personal data; or any personal data. Previous state laws have extended the right to obtain a list of categories of third parties to whom a consumer's personal data has been disclosed, but Oregon will be the first state to require production of a specific list of third parties upon consumer request. The Oregon Attorney General's office is expected to vigorously enforce this section (according to commentary made at a recent IAPP panel), so companies should ensure that they have ongoing, regularly updated, processes in place to (1) track and maintain a list of all third parties (including via third-party tracking technologies) to whom a consumer's (or all consumers') personal data is disclosed; and (2) provide that list to consumers upon request.
- **Texas:** The Texas Data Privacy and Security Act also takes effect July 1, 2024. One notable distinction from other state laws is the threshold for application of the law. All comprehensive state privacy laws in effect so far apply to entities based on some combination of an entity's gross revenue, the annual number of consumers whose personal data the entity

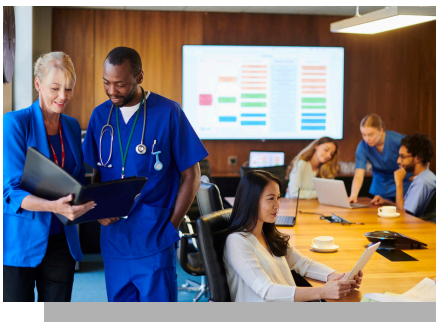
processes and/or sells, and/or the amount of revenue the entity receives from the sale of personal data. Based on that threshold, the law either applies in its entirety, or it doesn't apply at all to that entity. Conversely, Texas exempts all small businesses (as defined by the United States Small Business Administration) from its law, except that small businesses are still required to obtain consumer consent for the sale of sensitive data. Other (larger) entities are required to obtain consumer consent for all processing of sensitive data in addition to complying with the rest of the law. Texas also requires larger entities that sell sensitive data to include a reasonably accessible and clear privacy notice with the specific language: "NOTICE: We may sell your sensitive personal data."

- **Montana:** The Montana Consumer Data Privacy Act takes effect October 1, 2024, and is borrowed almost entirely from Connecticut's law. One notable distinction, however, is the threshold for application of the law. Montana follows the same structure for application of the law as other states (except Texas–see above), based on the number of consumers whose personal data the entity processes or the percentage of revenue from the sale of personal data. However, the numbers are lower, effectively making the law applicable to smaller businesses that may not be subject to privacy laws in other states. Specifically, Montana's law applies to entities that control or process the personal data of not less than: (a) 50,000 consumers (excluding data processed for completing a payment transaction); or (b) 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data. Connecticut, in comparison, has the same standard except with 100,000, instead of 50,000, consumers in the first part of the standard.

Washington and Nevada Consumer Health Laws Enter the Mix

Two state laws governing consumer health data took effect March 31, 2024 in Washington and Nevada.

- **Washington:** In addition to the geolocation aspects of the law (which took effect in 2023), Washington's My Health My Data Act (MHMD) will now require that covered entities comply with certain notice and consent requirements, and it will extend certain user rights, with respect to "Consumer Health Data". Conceptually, these elements are already present in several comprehensive state privacy laws. However, MHMD is notable for several reasons.



    - MHMD's definition of "Consumer health data" is broader than the "health data" portion of state-sensitive data definitions and likely encompasses a lot of information that would not fall under the "sensitive data" definitions of effective state comprehensive privacy laws.
    - MHMD prohibits the collection or sharing of consumer health data without consumer consent, and the MHMD consent requirements are more stringent than state "sensitive data" consent requirements.
    - MHMD covered entities will be required to place on their homepages a prominent link to a consumer health data privacy policy, separate and distinct from other policies.
    - Certain consumer rights must be extended that go above and beyond most comprehensive privacy laws.
    - Most notably, MHMD includes a private right of action, which is not present in any state comprehensive privacy laws to date with respect to similar requirements.

- **Nevada:** Nevada's Consumer Health Data Privacy Law resembles MHMD in some respects, but one major distinction is that the Nevada law does not include a private right of action. Additionally, the definition of Consumer Health Data (although still broad) is narrower than MHMD.

California and Connecticut Take Decisive Action on Enforcement

In Q1 2024, regulatory bodies in California and Connecticut have taken assertive steps to uphold privacy laws, marking a significant phase in privacy law enforcement.

- **California**
  - **AG's Investigative Sweep of Connected TV and Streaming:** In January, California Attorney General Rob Bonta's office initiated a CCPA compliance investigation targeting streaming services and connected TV providers, focusing on facilitating consumer opt-out rights. The AG's sweep signals that California regulators are focused on ensuring that companies provide functional and easy-to-use opt-outs, and that opt-out requests are honored across all companies' streaming platforms.

  - **DoorDash Settles with AG Over Data Sale Violations:** In February, DoorDash reached a settlement with the California AG for alleged violations of the CCPA and the California Online Privacy Protection Act (CalOPPA). The issue centered around the unauthorized sale of personal information through marketing cooperatives, which, despite lacking direct financial exchange, constituted a "sale" under the CCPA. The alleged failure of DoorDash to rectify its privacy policy and provide an opt-out mechanism after a 2020 notice of noncompliance was a key factor in the AG's decision. Regulators also found that even though DoorDash eventually stopped selling personal information, it could not cure its past violations because the company lacked the ability to ensure downstream recipients of personal information deleted it. The settlement mandated a $375,000 fine and the establishment of a comprehensive privacy program by DoorDash, overseen by audits for the next three years. This action is only the second public enforcement action under the CCPA, following Sephora's settlement with the AG in 2022.

- **Conneticut**
  - **Six-Month Enforcement Report:** Meanwhile, in Connecticut, the Office of the Attorney General (OAG) released a report discussing the first six months of enforcement of the Connecticut Data Privacy Act (CTDPA). The report focuses on privacy policy improvements, sensitive data protection, and data related to teens. With over a dozen investigations, Connecticut has emerged as a proactive enforcer of its privacy law. The report says that while progress has been made, challenges in enforcing the CTDPA persist, prompting the OAG to make several legislative recommendations to narrow the entity-level exemptions in the law and strengthen consumer rights.

CCPA Rulemaking Focus: Automated Decision-Making and Risk Assessments

In March, with a split vote of 3 to 2, the CPPA board voted to move forward with preparing draft regulations covering automat-

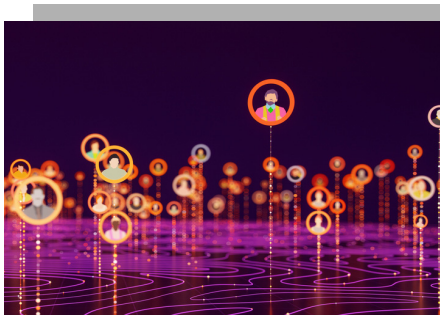
ed decision-making technologies (ADMT) and risk assessments. This means that the CPPA staff have been authorized to prepare materials necessary to publish a notice of proposed rulemaking. Staff estimated that the materials would be ready for a meeting in July 2024. At that time, the board will decide whether to start formal rulemaking. If the board decides to move forward with formal rulemaking, there will be a 45-day public comment period, and the CPPA will have 1 year to formalize the regulations. The board estimated that final regulations would not be ready until Q1 2025.

At the March meeting, the CPPA reviewed a revised draft of the regulations covering ADMT and risk assessments made available to the public in February. Below are some of the key changes from the prior draft.

- **Behavioral Advertising:** The draft introduces new risk assessment and ADMT obligations for "behavioral advertising," which is defined as the targeting of advertising to a consumer based on the consumer's personal information obtained from their activity across third party services and within the business's own services. Behavioral advertising expressly includes cross-context behavioral advertising, but does not include non-personalized advertising provided that the consumer's personal information is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business and is not disclosed to a third party. This definition is so expansive that it could be interpreted to require businesses to provide an opt-out for advertising using first party data (even if there is no sale or share). Such a broad interpretation could potentially impact measurement, attribution, and other services associated with advertising.

- **Physical or Biological Identification:** The draft introduces new obligations for businesses using physical or biological identification or profiling, including ensuring that such processing does not discriminate against protected classes. These requirements appear to be influenced by recent regulatory actions at the federal level regarding non-discrimination and biometrics, suggesting that regulators are influenced by each other in interpreting and enforcing consumer privacy.

- **Exceptions and Human Appeal:** The draft includes new exceptions for workplace and security issues and introduces a human appeal exception, allowing businesses to offer a human review process instead of a direct opt-out option.



As a reminder, the draft includes the following key requirements for businesses using ADMT:

- **Pre-Use Notice Requirement:** Under this requirement, businesses must inform consumers about the ADMT's purpose, opt-out rights, access rights, and how the ADMT operates. Notices must be prominent and explain any exceptions to rights. Exceptions for ADMT use in security, fraud prevention, safety, or training are narrow and specific.

- **Opt-Out Requirement:** Under this requirement, consumers have the right to opt-out of ADMT processing of their personal information. Businesses must stop using ADMT on a consumer's personal information within 15 business days after receipt of an opt-out, and must notify downstream recipients. Businesses must offer an interactive form and an additional opt-out method, without requiring an account or verification. New exceptions include limited cases for workplace and public profiling, and a "human appeal" option for decisions made by ADMT (as noted above).

- **Access Right Requirement:** Under this requirement, consumers have the right to request details on how their personal information was used by ADMT. Businesses must provide specific information about the ADMT's use, its output, and how the consumer was affected. Exceptions exist for ADMT use in security, fraud prevention, or safety, or data used solely for training.