

March 2025

Follow us on [LinkedIn](#) 

## Legislative Update

# US Privacy Update: Where Things Stand at the Start of Q2 2025

By [Aaron Charfoos](#), [Michelle A. Reed](#) and [Jeremy Berkowitz](#)

Three months into 2025, there appears to be no slowdown in the flood of privacy legislation being considered and enacted by both Congress and state legislatures. Since the California Consumer Privacy Protection Act was passed in 2018, more than two dozen states have passed state privacy laws. While Congress has also made attempts to upgrade existing federal privacy laws, it has generally been unsuccessful so far.

### Federal Privacy

#### Federal Comprehensive Privacy Bill

In the past four years, Congress tried twice to pass a federal privacy law. In 2022, the American Data Privacy and Protection Act, which would have established national privacy standards preempting most state privacy laws, was passed out of the House Energy and Commerce Committee but never received a vote in the full House or the Senate. In 2024, House Energy and Commerce Committee Chair Cathy McMorris Rogers (R-WA) and Senate Commerce Committee Chair Maria Cantwell (D-WA) introduced a similar bill, the American Privacy Rights Act, but were never able to get traction from their counterparts in the House and Senate to consider the bill. There has been a change in committee leadership this Congress, but it is unclear whether new House Energy and Commerce Committee Chair Brett Guthrie (R-KY) and Senate Commerce Committee Chair Ted Cruz (R-TX) have the desire or bandwidth to make another attempt at a federal privacy bill, given their oversight of other issues and the busy congressional calendar.

#### Federal Children's Privacy

One area where Congress has come to a legislative consensus is upgrading laws around children's privacy. The Kids Online Safety Act (KOSA) passed the Senate last year by a wide margin but never received a vote in the House. KOSA, which congressional leaders are expected to reintroduce in this Congress, is aimed at enhancing online protections for minors by requiring platforms to implement safeguards, restrict harmful content and provide greater parental controls of their children's data. The bill builds upon existing children's privacy laws, including the 1998 Children's Online Privacy Protection Act, and is part of broader efforts to regulate social media and digital platforms.

Key provisions of KOSA include:

- **Establish a Duty of Care for Online Platforms**
  - Requires social media companies, gaming platforms and online services to act in the best interest of minors by preventing exposure to harmful content (e.g., self-harm, eating disorders, drug use, online exploitation).
  - Platforms must conduct regular risk assessments on how their algorithms and design choices impact young users.
- **Enhanced Parental Controls and Age Verification**
  - Requires default parental controls on accounts for all users under 16.
  - Platforms must provide tools for parents to monitor screen time, restrict certain content and adjust privacy settings.
- **Restricting Algorithmic Targeting of Minors**
  - Prohibits platforms from using recommendation algorithms to serve content that could harm minors' mental or physical well-being.
  - Gives minors and parents the ability to disable algorithm-driven content feeds.
- **Transparency and Data Access**
  - Requires platforms to provide public reports on risks to minors and their efforts to mitigate them.
  - Grants independent researchers access to platform data to study the effects of social media on children's well-being.
- **Limitations on Data Collection and Targeted Ads**
  - Bans targeted advertising to users under 16.
  - Prevents platforms from collecting, using or sharing children's personal data beyond what is necessary for platform functionality.

The Federal Trade Commission (FTC) and state attorneys general would have the ability to enforce KOSA.

## State Privacy

There continues to be a flurry of activity in the states to both introduce and amend new privacy laws. These laws run the gamut from new comprehensive state privacy laws to more targeted legislation. Here are some general themes of the state legislation, along with specific examples from states.

### Comprehensive Privacy Bills

Eight states had comprehensive privacy legislation that went into effect prior to the start of this year: California, Colorado, Connecticut, Montana, Oregon, Texas, Utah and Virginia. Six states have comprehensive bills that have gone into effect, or are going into effect, this year: Delaware, Maryland, Minnesota, New Hampshire, New Jersey and Tennessee. Each law has its own distinctions. For example, New Jersey and Maryland both have unique definitions around data classification and minimization.

**New Jersey:** The New Jersey Data Privacy Act classifies all financial information as sensitive data. The law states that sensitive data may not be processed without the express consent of individuals. Additionally, while the bill would allow companies who are governed by the Gramm Leach Bliley Act to claim an exemption, it only allows companies to take a Health Information Portability and Accountability Act (HIPAA) exemption at the data level, meaning that companies must abide by the law for their non-HIPAA related data.

**Maryland:** The Maryland Online Data Privacy Act strictly prohibits the sale of sensitive data and strictly regulates the sale of other types of personal data. It also introduces data minimization standards in its law, strictly requiring companies that collect personal data to only process it for the purposes they have told their customers.

Fourteen other states are in the process of debating comprehensive state legislation. For example, Massachusetts and Vermont are imposing new requirements on the processing of personal data:

**Massachusetts:** The Massachusetts Data Privacy Protection Act, currently being debated in both legislative bodies, like the Maryland bill would set data minimization standards. It also prohibits the sale of sensitive personal data.

**Vermont:** Vermont is making a second attempt to pass a privacy bill after the governor vetoed a bill last year passed by the legislature. The Vermont Senate is proposing a bill that would require opt-in consent for processing of all sensitive data, which it is defining as including biometric data. It would require that sensitive data only be collected if strictly necessary for providing a service and also would permit a private right of action as it relates to processing of sensitive data.

#### State Children's Privacy Legislation

Many states are introducing bills that model KOSA. There is a particular focus on protecting children's data from social media companies, and many of these proposed laws are requiring online platforms and app stores to implement age verification systems and require parental consent before minors can access certain digital services. Additionally, some of these bills are regulating minors' access to social media by imposing age restrictions, account termination policies and parental supervision tools.

As an example, Alabama is currently debating several bills that would require app store providers to verify ages and obtain parental consent for minors' data processing, as well as impose age restrictions on access to these sites. They would also require social media platforms to terminate certain accounts and provide tools for parents to oversee what their children are doing on these platforms.

Some states are also seeking to propose strict rules on collecting, using and selling children's data. Some of these proposed laws prohibit targeted advertising to minors or require companies to minimize the data they collect. As an example, Arkansas is considering legislation that requires parental consent for the ability to sell their children's data and/or use it for targeted advertising.

Some states are pushing for regulations that limit children's exposure to harmful content and require platforms to remove inappropriate material. Some of these laws are also requiring online services to set privacy-friendly defaults for minors, such as restricting adult communication, disabling tracking and preventing addictive features.

As an example, California is considering legislation that would reinforce existing laws requiring websites to allow minors to remove their posted content. This is in addition to California's Age-Appropriate Design Code Act (CAADCA), passed in 2022, which requires that digital products and services be designed with the well-being of children in mind and that privacy settings in services or products likely to be accessed by children be set to the highest level by default. The CAADCA is currently held in federal court by legal challenges. Additionally, Oklahoma is considering legislation that would require platforms to limit data processing, block profiling and set default privacy protections for minors.

### Biometric Privacy Legislation

Three states (Illinois, Washington and Texas) currently have comprehensive biometric privacy laws to regulate the collection, storage and use of biometric data, such as fingerprints, facial recognition data and retinal scans. These laws focus on protecting individual privacy, requiring consent and imposing restrictions on businesses and government agencies that handle biometric data.

Missouri is the latest example of a state considering a biometric privacy law. The proposed Missouri Biometric Information Privacy Act, which has been introduced in both of its state legislative bodies, would require written consent from an individual before collecting biometric information and identifiers. The bill also establishes a private right of action and requires that companies only keep the biometric data for necessary purposes or dispose it after one year, similar to Texas's law, but stricter than the three years permitted under Illinois law.

Some states are seeking to regulate the misuse of biometric data by certain technologies. As an example, Massachusetts is considering a bill that would focus on regulating government use of biometric recognition technology. Additionally, Minnesota is considering a bill regulating the use of brain technology to manipulate stimuli and ensuring affected individuals provide consent for the use of such technology, as well as requiring doctors and hospitals provide notice on how they use the data and how long they can store it for.

### Health Privacy Legislation

Proposed health data privacy laws in 2025 focus on protecting individuals' medical information, limiting data sharing and enforcing transparency in health-related data collection. These laws aim to ensure patient consent, restrict unauthorized disclosures and regulate digital health services.

Some states are introducing bills modeled after the state of Washington's My Health My Data Act, a law passed in 2023, that requires explicit consent from individuals before collecting, sharing or processing health information, including data related to an individual's reproductive health rights. States are also banning the sale of health data to third parties, including advertisers and data brokers. Some bills introduce stricter security mandates and require companies to notify individuals in case of a health data breach. For example, New Mexico and New York are considering bills mandating that entities handling health data obtain individual consent before use. New York is also considering separate legislation that would mandate express written consent before filming or sharing a patient's medical treatment data. Illinois has also introduced legislation prohibiting the sale of sensitive health data.

Other states are introducing new rules for mobile health apps, telemedicine platforms and online health data storage. As an example, Montana is establishing confidentiality standards for mental health digital services, requiring secure data handling.

In summary, even without a comprehensive federal privacy law on the horizon, it is likely that 2025 will be a busy year in this space, as states look to follow their counterparts and provide regulations and guidance on upcoming privacy risks. Paul Hastings will keep you updated regarding progress of this activity and how it could potentially affect your businesses.



---

*If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:*

**Chicago**

Aaron Charfoos  
+1-312-499-6016  
[aaroncharfoos@paulhastings.com](mailto:aaroncharfoos@paulhastings.com)

**Dallas**

Michelle A. Reed  
+1-972-936-7475  
[michellereed@paulhastings.com](mailto:michellereed@paulhastings.com)

**Washington, D.C.**

Jeremy Berkowitz  
+1-202-551-1230  
[jeremyberkowitz@paulhastings.com](mailto:jeremyberkowitz@paulhastings.com)

**Paul Hastings LLP**

Stay Current is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2025 Paul Hastings LLP.