Articles + Publications | November 10, 2025

Retrospective: 2025 in State Data Privacy Law

WRITTEN BY

David M. Stauss

This article was originally published on IAPP and is republished here with permission as it originally appeared on November 10, 2025.

Although 2025 may end as the first year since 2020 in which no new state comprehensive privacy law is enacted, this year was anything but quiet. We saw hundreds of consumer privacy bills introduced, newly enacted amendments to existing laws, multiple states engaging in rulemaking, including potentially game-changing rulemaking in California, new sectoral laws addressing health and youth privacy and online safety, and an uptick in state enforcement activity.

No new comprehensive laws: A turning tide?

For the first time since 2020, we may not see any new state comprehensive privacy laws enacted this year. This lack of activity is conspicuous and enigmatic. This could be a natural consequence of diminishing marginal returns if the states that were most likely to enact privacy legislation have already done so. It could be simple bad luck, given how unpredictable the legislative process can be.

Bills in Alabama (HB 283), Oklahoma (SB 546) and Georgia (SB 111) all stumbled at the final steps. Given other events happening at the local, state, federal and global levels, state lawmakers could have had more pressing legislative priorities than privacy this year. Or the content of the bills themselves could have diminished the likelihood of passage, as multiple states considered diverging models from the status quo. Legislators in Maine (LD 1822) and Vermont (H208) once again considered bolder, more-restrictive frameworks, but neither state got as close this year as they did in 2024.

It remains possible that 2025 could see a new comprehensive privacy law sneak in just before the turn of the year. Massachusetts is making a late push — S2619 passed the Senate by a vote of 40 to 0 on 25 Sept. — but they are working against the clock. That is a Maryland-style bill characterized by the inclusion of strict, substantive data minimization requirements. Pennsylvania is another late mover — HB 78 passed the House 1 Oct. A similar bill passed the Pennsylvania House last year but stalled in the Senate. Michigan (SB 359) and Wisconsin (AB 172) both have active legislative sessions at the time of writing, but neither have progressed a bill out of committee.

The amendment era: 9 states tweaked existing privacy laws in 2025

There might have been a slowdown in new laws this year, but 2025 was very active for amendments to existing laws as nine states amended their existing comprehensive privacy laws. This year's crop of amendments include a mix of states incorporating existing aspects of other states' laws and states experimenting with novel provisions.

One of the more significant amendments this year was Sen. James Maroney's, D-Conn., SB 1295, which overhauled Connecticut's comprehensive privacy law yet again. The themes of the amendment were expanded coverage, expanded consumer rights, tightened restrictions with respect to minors and integrating AI-related provisions. The amendment adjusted the law's applicability thresholds, expanding coverage to include entities who control or process the personal data of at least 35,000 consumers, control or process consumers' sensitive data, excluding personal data controlled or processed solely for completing a payment transaction, or offer consumers' personal data for sale.

The amendment also replaced the law's entity-level Gramm-Leach-Bliley Act exemption with a data-level exemption, although that change was counterbalanced by new entity exemptions for certain insurers, banks and investment agents. The definition of "sensitive data" was also expanded, and now includes financial data and neural data. The consumer right to access one's personal data was expanded to include inferences derived from one's personal data and whether personal data is being profiled to make decisions with legal or similarly significant effects. SB 1295 added new rights as well — a right to know the third-party recipients of one's personal data and a right to contest certain adverse profiling decisions. The amendment also tightens the protections for minors added by SB 3 in 2023. Among the changes is a complete prohibition on targeted advertising to minors under age 18.

The bill also creates a new approach to profiling and impact assessments. It expands the right to opt-out to apply to all automated decisions, not just "solely" automated decisions. Consumers also have a new right to question profiling results under some circumstances. Further, controllers that engage in profiling for the purpose of making a decision that produces any legal or similarly significant effect concerning consumers must conduct an impact assessment. Ultimately, given the law's entity- and data-level exemptions, it remains unclear whether these changes will have a significant impact on businesses. Finally, in a first for a state privacy law, Connecticut also now requires controllers to provide a statement disclosing whether the controller collects, uses or sells personal data for the purpose of training large language models. The amendments go into effect 1 July 2026.

Another significant change came in Montana. Two years on from the Montana Consumer Data Privacy Act's first enactment, Montana Sen. Daniel Zolnikov, R-Mont., returned with a significant update to his law. Among the changes made by SB 297 are increased applicability, now applying to persons that either control or process the personal data of at least 25,000 consumers, or control or process the personal data of at least 15,000 consumers if the controller derives at least 25% of gross revenue from the sale of personal data), a duty of care with respect to minors — similar to amendments in Connecticut and Colorado in 2023 and 2024 — and broadened enforcement power for the attorney general, including removing the right to cure.

The other states made less significant changes to their laws. The Oregon Consumer Privacy Act was amended three times: HB 2008 bans the sale of precise geolocation data and personal data of consumers under age 16; HB 3875 expands the law's applicability to include motor vehicle manufacturers and affiliates who control or process any personal data obtained from a consumer's use of a motor vehicle or a component of a motor vehicle; and SB 1121 modifies the right to cure. In Colorado, SB 25-276 added "precise geolocation data" (1,850 feet) as a category of sensitive data, bringing Colorado into alignment with most state comprehensive privacy laws. SB 25-276 also clarified that selling sensitive data requires opt-in consent.

The Kentucky Consumer Data Protection Act was also amended by HB 473 before it even went into effect. That

bill made minor conforming changes to the law, such as new health care data-level exemptions and a clarification that a data protection assessment should be conducted for the processing of personal data for the purposes of profiling where the profiling presents a reasonably foreseeable risk of "unlawful, disparate impact on consumers," not just disparate impact on consumers.

The Texas Responsible Artificial Intelligence Governance Act, although largely focused on government use of AI, made minor changes to existing privacy laws. This act added new language regarding contracts between controllers and processors under the Texas Data Privacy and Security Act, requiring processors to assist controllers in complying with requirements relating to the personal data collected, stored and processed by an AI system.

It also amends the Texas Capture or Use of Biometric Identifier Act by adding an exemption for developing or deploying AI systems that are not used to uniquely identify specific individuals; adding an exemption for developing or deploying AI systems used for certain security purposes; and clarifying that individuals do not consent to the capture or storage of biometric identifiers due to the presence of publicly available media online unless that image or media was made publicly available by the individual.

New social media restrictions were added to the Virginia Consumer Data Protection Act by SB 854, now requiring operators of social media platforms to use "commercially reasonable methods" to determine whether users are minors and to limit minors' use of the platform to one hour per day (or more or less with parental consent). Finally, the Utah Consumer Privacy Act was brought further into alignment with other states when HB 418 added a right for consumers to correct their personal data.

Last but not least, California passed the Opt Me Out Act. This bill amends the California Consumer Privacy Act to require any business that develops or maintains a browser to include a setting that is easy to locate and use which enables a consumer to activate an opt-out preference signal. A browser is defined as an interactive software application used by consumers to locate, access and navigate internet websites. Readers may remember that Gov. Gavin Newsom, D-Calif., vetoed a similar bill last year, citing concerns over how that bill would have applied to mobile operating systems. This year's bill was narrowed to focus exclusively on browsers.

Activity shifts from legislation to regulations

Perhaps the biggest story coming out of 2025 is California's new CCPA rulemaking. The California Privacy Protection Agency's rulemaking covers automated decision-making technology, risk assessments, cybersecurity audits, insurance requirements and updates to the existing CCPA regulations. The regulations go into effect 1 Jan. 2026, although the ADMT, risk assessment and cybersecurity audit regulations have staggered implementation deadlines. Notably, the risk assessment and cybersecurity audit regulations will, starting in 2028, require businesses to submit certifications to the CPPA attesting, under penalty of perjury, that the regulations' requirements have been met. That novel approach — at least in the realm of state consumer data privacy laws — will no doubt drive significant compliance activities.

The final redline of the regulations is 127 pages long, covering a long list of topics and nuances that are beyond the scope of this article. However, one area that warrants some mention is the ADMT regulations, which were the subject of extensive — and often passionate — comments and revisions during the drafting process. The ADMT

regulations also were promulgated during a global shift in approach on artificial intelligence regulation towards a more innovation-friendly environment.

The CPPA Board and staff significantly revised ADMT regulations during the rulemaking process. Ultimately, businesses that use ADMT for certain types of significant decisions such as lending, housing, education or employment, in a manner that replaces or "substantially replaces" human decision-making, a defined term, will need to provide notices, allow for an opt-out, or right to appeal, provide a right to access ADMT, and conduct risk assessments.

Meanwhile, over 1,000 miles east, the Colorado attorney general's office amended the Colorado Privacy Act rules in three ways. First, the office operationalized the children's privacy law amendments passed in Sen. Robert Rodriguez's, D-Colo., SB 41 by providing direction for what it means for a controller to "willfully disregard" that a consumer is a minor — under age 18. Second, the amendments fleshed out what it means for a system design feature to significantly increase, sustain or extend a minor's use of an online service, product or feature. Finally, the amendments changed the rule's existing definition of "revealing" to address the addition of precise geolocation data as an element of sensitive data in the law's 2025 amendment discussed above.

Finally, moving east another 1,700 miles, New Jersey entered the rulemaking fray. When the New Jersey Data Privacy Act was enacted last year, much ado was made about it being only the third law to include general rulemaking authority. In June, the Division of Consumer Affairs released long anticipated draft regulations. Although the draft largely copied Colorado's existing regulations, there were a few novel aspects that drew intense scrutiny. For example, the draft departed from existing legal frameworks by proposing a definition of publicly available information that excluded scraped data, although no definition of scraping was provided.

The draft also took a novel approach to the law's internal research exception, providing that the exception did not apply to using personal data to train AI systems without consumers' consent. "Artificial intelligence" was yet another key undefined term. Public feedback concluded in August, and we await to see what changes the Division will make in response.

Enforcement: The gathering storm

2025 also witnessed an uptick in state enforcement activities. In California, the CPPA entered into a USD632,500 settlement with an automaker, a USD345,178 settlement with a clothing retailer, and a USD1,350,000 settlement with a rural lifestyle retailer. The CPPA also fined various data brokers for failing to register under the state's data broker registration law. Meanwhile, the California attorney general's office entered into a USD1,550,000 settlement with a health website publisher. In addition, Connecticut's attorney general's office fined an online ticketing marketplace USD85,000.

The nature of the enforcement actions primarily center around improper consumer disclosures, e.g., deficient privacy notices and deficient consumer request processes — predominantly the right to opt-out of selling/sharing and recognition of the Global Privacy Control signal. Other issues include failure to enter into data processing agreements, violation of the CCPA's purpose limitation provision and malfunctioning consent management platforms.

Although much of the focus on the enforcement actions has been on the size of the fines or types of violations, businesses would be wise to also focus on the injunctive relief provisions. For example, the most recent CPPA enforcement action required the company to conduct scans of its digital properties (at least quarterly) for the purposes of maintaining a full and current inventory of tracking technologies, identifying which tracking technologies constitute sells or shares and properly effectuating opt outs. The CPPA also has required regular audits and contract management processes. These injunctive relief provisions provide a potential roadmap for businesses to develop privacy program policies to demonstrate good faith compliance efforts in case of an enforcement action.

Of course, no discussion of state enforcement activity can be complete without talking about Texas. In contrast to the other states, Texas has taken a litigation-first approach to enforcement. This year, Texas entered into an over USD1 billion settlement with a tech company in a lawsuit that predates its consumer data privacy law. The Texas attorney general also filed a lawsuit against an insurance company and its subsidiary over allegations they violated Texas' consumer data privacy law, data broker law and insurance code.

Florida similarly joined the party of first-time enforcers this year. Whether the Florida Digital Bill of Rights is "comprehensive" remains controversial among privacy professionals, given the law's narrow applicability thresholds. Nevertheless, the attorney general's office recently announced a lawsuit against a content platform for connected televisions. The allegations largely concern the selling of sensitive data (including precise geolocation data and the personal data of known children) for targeted advertising without consent. The complaint faulted the company for not implementing "industry-standard user profiles to identify which of its users are children." Under the FDBR regulations, a controller "willfully disregards" a consumer's age, and hence has actual knowledge, if it "should reasonably have been aroused to question whether a consumer was a child and thereafter failed to perform reasonable age verification." The complaint points to a number of age signals that could have prompted an inference that children were using the service, including content designated as "Made for Kids." Another notable aspect of the lawsuit is the high civil penalties — up to USD150,000 per violation.

As more laws come into effect and right-to-cure periods expire, businesses should expect a new era of enforcement activity and they will soon likely be shifting their compliance activities from integrating new laws to integrating enforcement priorities. Indeed, the CPPA's head of enforcement, Michael Macko, recently caused quite a stir when he announced the CPPA had hundreds of open investigations. States also have shown a willingness to act together with California, Connecticut and Colorado announcing a joint investigative sweep and 10 states forming a Consortium of Privacy Regulators.

The chaos of kids' online data privacy laws

At least since California passed its Age-Appropriate Design Code Act in 2022, state lawmakers from both parties and across the country have been trying to find a way to regulate teen and children's data privacy and online safety. Last year, we discussed new laws enacted in Colorado, Maryland and New York. This year, we saw news laws passed in Arkansas, California, Louisiana, Montana, Nebraska, Texas, Utahand Vermont. As discussed above, there also were kids' privacy-related changes to Connecticut and Oregon's data privacy laws as well as rulemaking in Colorado. The CPPA's new regulations also revised the regulation's definition of sensitive personal information to include "[p]ersonal information of consumers that the business has actual knowledge are less than 16 years of age."

Arkansas' law stands alone for both its unique approach and its perplexity. Effective 1 July 2026, the law contains contradictory and ambiguous provisions. Meanwhile, Nebraska and Vermont passed age-appropriate design code acts; however, the laws are vastly different rendering the "AADC" moniker essentially meaningless. On the other hand, Montana amended its law to add children's privacy provisions similar to those enacted in Colorado and Connecticut. While this interoperability may have been a welcome sight for companies, Connecticut then amended its law to significantly revise these provisions. To add to the complexity, Louisiana, Texas, and Utah passed app store accountability acts, which (if they survive constitutional challenge) will require app stores to collect age information and send age bracket signals to app developers in addition to creating parental oversight of teen and child accounts. California passed a somewhat similar law that requires operating systems to collect age information and send signals to apps.

New laws and no enforcement contribute to continued uncertainty for health privacy

Consumer health has been one of the more volatile privacy legislative areas in recent years and 2025 continued that trend. January got off to a dramatic start as New York passed S929, the New York Health Information Privacy Act. The bill is currently stuck in legislative limbo, as it has not yet been transmitted to the governor for signature or veto. NYHIPA is similar in scope and substance to Washington's My Health My Data Act but introduces several novel requirements. For example, the bill includes a 24-hour waiting period before a regulated entity can request consent for a processing activity that is not strictly necessary for one of the law's permitted purposes, e.g., providing a requested product or service or complying with legal obligations. The bill notably lacks some common features of privacy bills, such as any provisions concerning the verification of consumer rights requests.

In one of the surprises of the year, Gov. Glenn Youngkin, R-Va., signed SB 754, a new health privacy requirement that prohibits obtaining, disclosing, selling or disseminating any personally identifiable reproductive or sexual health information without a consumer's consent. That bill amends the Virginia Consumer Protection Act rather than the Virginia Consumer Data Privacy Act, so it is subject to a private right of action. The bill quickly went into effect 1 July and has already raised compliance questions.

In California, two health privacy bills were enacted this year. Like many health privacy bills passed since the Dobbs decision, AB 45 introduces new restrictions on geofencing facilities that provide in-person health care services for certain purposes and collecting, using or disclosing the personal information of persons at family planning centers. That bill makes it unlawful to geofence such a facility, within a radius of 1,850 feet, for certain purposes, such as to identify or track a person seeking health care services or to send such a person advertisements related to their personal information or health care services.

The bill further prohibits persons from selling or sharing personal information to a third party for a use that violates any of those geofencing prohibitions. The bill includes an exception for geofencing your own health care facility to provide necessary health care services. A narrower bill, SB 81, amends the California Confidentiality of Medical Information Act to extend protections to certain immigration-related data. Both bills include restrictions on disclosing certain data to law enforcement agencies.

Finally, we continue to wait for enforcement of two landmark health privacy laws — Washington's MHMDA and Nevada's consumer health data law (Nev. Rev. Stat. § 603A.400 et seq.). Both laws went into effect more than a year ago on 31 March 2024, but we have yet to see any public enforcement. 2025 did see the first class-action

lawsuit claiming a violation of MHMDA, concerning the use of third party SDKs, but that case was consolidated in April with other SDK litigation and dismissed without prejudice in May.

Data brokers remain in regulatory focus

Data brokers continue to attract legislative scrutiny, particularly in California. Late last year, the CPPA finalized regulations concerning data broker registration pursuant to the Delete Act and kicked off a series of enforcement actions for failure to register as a data broker. The CPPA has engaged in several rounds of rulemaking under the law and is currently in the process of finalizing new regulations operationalizing the Delete Request and Opt-out Platform, a mechanism that will allow consumers to submit a single mass deletion request to registered data brokers. California also passed SB 361, amending the Delete Act, this year. That bill adds new categories of information that a data broker must provide when registering with the CPPA. These new disclosures mostly concern whether the data broker collects certain categories of consumers' personal information, e.g., Social Security numbers, sexual orientation status, precise geolocation or whether the data broker has, in the past year, shared or sold consumers' data to certain actors, such as, foreign actors, a state government, the federal government.

Texas also amended its data broker law — twice. One of the bills, SB 1343, marginally increases notice obligations, requiring data brokers to include information as to how consumers can exercise any rights they have under the TDSPA in their website's privacy notice and to include a relevant link in their registration. The other amendment, SB 2121, expands the law's coverage. "Data broker" is now defined as "a business entity that collects, processes, or transfers personal data that the business entity did not collect directly from the individual linked or linkable to the data." Previously, to qualify as a data broker an entity's principal source of revenue had to be derived from its collection, processing or transferring of personal data. The bill retains additional eligibility criteria based upon revenue or the number of affected consumers.

Conclusion

The state privacy landscape grows more complex every year, as do the underlying issues around societal welfare, economic competitiveness, data-driven harms, surveillance' and mass data collection. As we all continue to await a unifying federal privacy approach, state policymakers are likely to continue to push legislative and regulatory responses to these thorny problems.

Jordan Francis, CIPP/E, CIPP/US, CIPM is senior policy counsel for the U.S. Legislation team at the Future of Privacy Forum.

David Stauss, CIPP/E, CIPP/US, CIPT, FIP, is a partner at Troutman Pepper Locke.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber