Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Top Data Privacy & AI Developments Of 2025: Midyear Report

By **Allison Grande**

Law360 (July 14, 2025, 10:55 PM EDT) -- The rise and rapid fall of a federal proposal to ban states from regulating artificial intelligence for a decade and an uptick in activity from data privacy enforcers in states across the country dominated headlines in the first half of 2025, and attorneys are expecting these areas to continue to grab attention in the coming months.

During the past six months, states from California to Connecticut have been building up their resources to focus more closely on how companies use and share consumer data, and the resounding demise of a congressional push to halt a growing AI patchwork only promises to make these states more central and active on these issues, attorneys say.

"This has been a common occurrence, with Congress trying to set a federal standard and states wanting to be autonomous and control their own fate," said Tara Cho, the chair of the privacy and cybersecurity team at Womble Bond Dickinson. "Now, with states continuing to enforce not just privacy but AI as well, we all have to buckle up for what will continue to be a scattershot approach to regulation."

AI Moratorium Out, State Regulations In

A sweeping proposal to withhold certain broadband funding from states that continued to enact and enforce laws to regulate emerging AI systems that surfaced in federal budget reconciliation negotiations earlier this year and seemed poised to pass late last month, after key Republican lawmakers struck a deal to reduce the length and potential scope of the ban.

But the tides quickly turned, with Sen. Marsha Blackburn, R-Tenn., backing down from the deal the following day, resulting in the Senate throwing its support behind an amendment co-sponsored by Blackburn to strip the proposed 10-year AI moratorium from the reconciliation package in a decisive 99-1 vote on July 1.

"It's clear we're living in a time where there's a lot of interest in the Trump administration and from leadership in Congress for a more deregulatory approach to AI," said Cobun Zweifel-Keegan, managing director at the International Association of Privacy Professionals. "This latest efforts highlights what this deregulatory movement could look like when it comes to state AI governance and emphasizes that this topic isn't going anywhere."

At the same time, the nearly unanimous rejection of the proposed moratorium also drives home "that not everyone is on the same page about the scope and scale of how AI should or should not be limited,"

Zweifel-Keegan noted.

Those pushing the AI ban — which included Senate Commerce Committee Chair Ted Cruz, R-Texas, and groups such as the Center for Data Innovation — had argued that the measure was necessary to avoid a complex patchwork of state regulations on AI and to allow for the innovation necessary to make the United States a global leader in this space.

"AI is advancing quickly, and policymakers should adapt accordingly — but not rush into regulation based on speculative fears," Center for Data Innovation Director Daniel Castro said in a July 2 post detailing five reasons "why critics were wrong" about the proposed ban and urging Congress to "revisit" the measure. "A 10-year moratorium gives Congress the time to study the technology, understand its implications, and focus on real harms rather than hypothetical ones."

Those who objected to the measure, including a bipartisan coalition of state attorneys general, dozens of consumer advocacy groups and the top Democrat on the Senate Commerce Committee, have countered that Congress' inability to put in place a nationwide framework to govern AI systems and models makes it imperative that states be allowed to establish regulations to protect consumers from bias, identity theft, data misuse and other potential harms posed by the rapidly developing technology.

"Congress should not prohibit states from protecting their residents when it comes to AI — especially without offering any alternative protections," Grace Gedye, policy analyst for AI issues at Consumer Reports, said in a July 1 statement. "Future legislation from Congress should not undermine state efforts; it should complement existing laws and learn from the laboratories of democracy."

Policymakers on both sides of the aisle also warned about the scope of the proposal, which they contended would reach existing and necessary consumer protections for activities such as automated decision-making and profiling done by AI systems and the use of AI to mimic performers.

"While companies' desire to have a more uniform set of rules is understandable, the moratorium had the potential to become incredibly confusing and cause a lot of litigation as everyone tried to figure out what state laws were covered, especially considering how much AI touches," said Hope Anderson, a partner in the data, privacy and cybersecurity practice at White & Case LLP.

With the AI moratorium dead for now, and no signs that Congress is working on federal legislation that would pass anytime soon, attention again turns back to the states, where hundreds of proposals have been floated to regulate some aspect of AI across every U.S. state.

"We're seeing a patchwork emerge in AI that's similar to what we've seen in the data privacy arena, where there are currently 20 different state laws that impact companies and make it challenging for them to keep up and build a scalable compliance program," said Kyle Kessler, a privacy and cybersecurity partner at Womble Bond.

Colorado and Texas currently lead the way as the only states so far to have put in place comprehensive frameworks for regulating the development and deployment of AI systems.

Colorado was the first to take this step with the passage of its AI Act last May. However, in signing off on the legislation, Democratic Gov. Jared Polis expressed reservations about the impact that the proposal to regulate certain high-risk AI system would have on innovation, similar to the concerns that caused Virginia's governor to veto comprehensive AI legislation earlier this year.

Polis urged the state Legislature "to work closely with stakeholders to craft future legislation for my signature that will amend this bill to conform with evidence based findings and recommendations for the regulation of this industry" before the law takes effect on Feb. 1, 2026.

"With the state AI moratorium now out of play, the question about whether there will be a special session for the Colorado Legislature to make changes or delay the bill are more apt than ever," said Tyler Thompson, a Denver-based partner in the emerging technologies at Reed Smith LLP.

Other states will likely pay close attention to how the debate in Colorado unfolds as they weigh how to regulate the topic in their own jurisdictions, Thompson predicted.

"Colorado is going to be the linchpin," Thompson said. "If the Legislature comes back and decides to make some improvements to the law, we could see a wave of other states follow that lead and pass comprehensive AI legislation. But if they don't get this fixed and the Colorado AI Act isn't enforced, that could be viewed as a failure and might scare off other states from enacting comprehensive AI laws in the future."

Texas, whose attorney general has been ramping up its data privacy and AI enforcement activities in recent months, also "stepped up even further to the privacy and AI plate" last month when its Republican Gov. Greg Abbott signed the Texas Responsible Artificial Intelligence Governance Act, noted Cynthia Cole, a partner in the data and cyber practice at Baker McKenzie.

While the law, which is slated to take effect on Jan. 1, was narrowed during the legislative process, the measure still imposes a comprehensive regulatory framework for those that develop or deploy AI systems available to Texas consumers, focusing specifically ensuring transparency regarding the technology's risks and prohibiting certain egregious uses of AI.

"The passage of the AI governance act in Texas shows that there's an interest in some level of responsible AI guardrails at the state level, even if that law is somewhat diminished from what we've seen in Colorado," said IAPP's Zweifel-Keegan.

California has taken a more piecemeal approach to AI regulation, enacting several separate laws addressing topics such as safety, misinformation and transparency, while Connecticut has also made strides by amending its data privacy law last month to require companies to disclose when they are using personal data to train large language models.

Additionally, companies that do business outside the U.S. will have to contend with a stringent new framework in the European Union to regulate high-risk AI systems, after the European Commission earlier this month denied a bid by several tech giants to delay implementation of the regulations by at least two years due to their complexity.

"We're seeing lawmakers work out in real time the challenges of balancing the need for strong regulation to address some very significant and real harms with a desire to allow companies to be competitive and not cut them off from innovating in this fast-moving AI space," said Anderson.

States Take Different Approach to Data Privacy

Following several years of states steadily adding comprehensive data privacy laws to the books, there

were no such statutes enacted in the first half of 2025. But that doesn't mean that states weren't active, with several jurisdictions moving to update their existing rules and boost protections for minors online.

"It's been a different kind of year in terms of state privacy law," said Zweifel-Keegan. "We haven't seen new comprehensive laws, but we have seen tweaks to established bills as well as new legislation on recurring themes such as health privacy, biometric privacy and kids' safety."

Connecticut, Montana, Oregon and Colorado have all moved to strengthen their data privacy frameworks, broadening protections for minors and precise geolocation data, lowering applicability thresholds and boosting transparency requirements, among other things.

"We're at the point where states are thinking through what works best for them in terms of data privacy and tweaking their laws to either conform to the mean or to innovate and be a little different or more aggressive than other states," Zweifel-Keegan said, adding that the attention being paid to comprehensive data privacy laws by both sides may be "freezing up" these efforts and pushing lawmakers toward narrower issues like the protection of sensitive information and kids' privacy.

In Connecticut, which put its sweeping data privacy law on the books in 2022, the state's Democratic governor last month signed legislation to not only raise the threshold for covered entities but also to expand what qualifies as sensitive data to include categories such as neural data and treatment and disability status; create new privacy notice requirements; and raise the age for heightened protection of minors to 17 from the current 16.

Oregon's governor similarly signed off on legislation in early June updating its data privacy regime to make it the second state, after Maryland, to ban the sale of precise geolocation data, a move that came on the heels of Colorado policymakers in May revising the definition of sensitive information in the state's data privacy law to include precise geolocation data and make clear companies can't sell people's sensitive information without first obtaining consent.

States have also dialed up their efforts in recent months to shield minors from online harms, with Texas, Vermont, Nebraska and Minnesota taking aim at this topic.

Both Vermont and Nebraska enacted their own Age-Appropriate Design Code Acts requiring social media providers to bolster data privacy and safety protections for children.

The Vermont law, which requires online services that children are "reasonably likely to access" to take steps to ensure that they're not using "abusive or privacy-invasive" design features or practices, hews closer to similar efforts to establish heightened protections for children online in California and Maryland that are facing First Amendment legal challenges, while the Nebraska law omits more controversial elements such as an explicit age verification requirement and obligation to conduct risk assessments.

Texas this year also became the second state, behind Utah, to require app stores to verify the age of individuals who create an account with the store, while Minnesota broke new ground with its own legislation mandating that mental health warning labels be displayed on social media platforms each time a user visits the site.

Kessler, the Womble Bond partner, noted that concerns over the potential loss of these state-level protections for minors appeared to be one of the driving forces behind the federal AI moratorium's

demise earlier this month.

"This priority being placed across the board on teens' and children's interests is something we're going to continue to see," Kessler said. "How minors are interacting with technology carries a lot of weight, and states will keep pushing to regulate this issue."

Privacy Enforcers Starting to Heat Up

While the comprehensive data privacy law landscape has yet to expand this year, several existing statutes have come into effect in recent months bringing enhanced powers for state attorneys general, who are already beginning to flex their new muscles.

"Generally, we are seeing more privacy and security regulation ... and regulations with very specific motivation to try to stop or change data behavior," said Cole, the Baker McKenzie partner. "We used to just talk about how the state privacy laws created complications for business, but now we have more than just state privacy laws to balance — we have increased state and federal regulation in various sectors and contexts, and that has created an increasingly complex privacy compliance web."

Within the past six months, the California Privacy Protection Agency — the nation's only stand-alone data privacy regulator — announced its first two enforcement actions under the state's data privacy law against American Honda Motor Co. and national clothing retailer Todd Snyder Inc., while the state's attorney general signaled he's still paying close attention to this space with the issuance of his largest data privacy settlement to date, against medical information provider Healthline Media LLC over its alleged failure to allow website visitors to opt out of targeted advertising.

"The Heathline decision is really a wake-up call in not only the healthcare space but for every website publisher out there that the California attorney general is worried about the protection of consumers' privacy and that they need to make sure that their opt-out mechanisms are configured correctly," said Heather Egan, a cybersecurity and privacy partner at Morgan Lewis & Bockius LLP.

Connecticut's attorney general also recently announced his first monetary penalty under the state's comprehensive data privacy law, against online ticket marketplace TicketNetwork.

And Texas Attorney General Ken Paxton, who last year set up a team dedicated to enforcing the state's consumer protections, continued building on these efforts by taking his first public action under the state's comprehensive privacy law in January. In that case, Paxton filed a lawsuit accusing insurance giant Allstate Corp. and its subsidiary Arity of unlawfully collecting drivers' location data through tracking software embedded in their mobile apps and then using that information to set car insurance rates.

Paxton has also moved to warn several companies with ties to the Chinese government, including AI startup DeepSeek, that their privacy practices likely aren't compliant with the state's data privacy law.

These enforcement efforts "drive attention to compliance and almost elevate the privacy laws in those states," White & Case's Anderson noted.

"Even if a certain state privacy law is not as restrictive as another state, once we start to see enforcement, that elevates those laws over other states," Anderson said.

Moving forward, Cole noted, it will be important as efforts mature to keep tracking the enforcement priorities of these regulators, many of whom have publicly confirmed that they're hiring more staff and otherwise expanding their resources to focus even more on this data privacy work.

"Some regulators are just getting started in earnest, and I am watching the patterns that are taking shape," Cole said.

--Editing by Alanna Weissman and Jay Jackson Jr.
