Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

States Pile On Privacy Law Patchwork As Congress Stagnates

By **Allison Grande**

Law360 (May 5, 2023, 10:55 PM EDT) -- A new consumer privacy law in Indiana, along with measures in three other states that are on the brink of enactment, take similar approaches to regulating the use and disclosure of personal data, but vital nuances are intensifying the need for a federal framework — even as that goal is looking increasingly elusive.

Indiana became the seventh state to enact comprehensive data privacy legislation on May 1, when its governor signed the Indiana Consumer Data Protection Act. That landscape is set to soon swell to double digits, with the legislatures in Florida, Montana and Tennessee approving similar measures within the past two weeks that are currently awaiting their governors' signature.

Like their predecessors, the four new measures are premised on principles that require businesses to give consumers the ability to access, delete, correct and stop the sale and sharing of their personal information. But they also contain differences in who they cover and how to implement these new consumer rights, complicating compliance efforts for the growing universe of companies that are being swept up by these measures.

"The more these laws occur and have nuances among them, the harder it becomes for businesses of a certain size that hold a certain amount of consumer data to comply with all these various laws and alert the public to their nuanced rights under these laws," said Sarah Hutchins, a partner and leader of the cybersecurity and data privacy team at Parker Poe Adams & Bernstein LLP. "So that continues to beg the question: Will companies get relief at the federal level?"

Since California became the first state to enact consumer privacy legislation in 2018, pressure has been mounting on Congress to head off a hodgepodge of laws by enacting a federal privacy standard.

The House Commerce Committee took a major step forward last year when it easily advanced the bipartisan American Data Privacy and Protection Act, which would give consumers a way to access, delete, correct and opt out of sharing the data companies hold on them; provide enhanced data protections for children; establish strong security standards; and allow consumers to bring private lawsuits after notifying certain state and federal regulators. But the proposal stalled on the House floor due to opposition — largely from California's congressional delegation — to the bill preempting more stringent state privacy law protections.

Meanwhile, states have continued to enact their own protections, with Virginia and Colorado putting laws on the books in 2021, Utah and Connecticut following suit last year and Iowa finalizing its own framework in March.

While the California law is largely seen as an outlier due to its unique features such as allowing consumers to sue on a limited basis and having its own dedicated agency to enforce the law, the other states have generally taken similar approaches to how they expect companies to disclose their practices and offer these rights to consumers.

"We're seeing something of a consistency across states now," said David Saunders, a partner at McDermott Will & Emery LLP. "There are a lot more similarities with these newer laws to one another than we saw from the California law to Virginia, which is good because that brings a clearer understanding of what companies' obligations are and what rights consumers are getting."

But while these similarities are helpful, they're not absolute.

"The legislatures just can't help themselves, and there's always a little something different from state to state, whether it's the applicability threshold or time for responding to consumer inquiries, which complicates matters and requires businesses to do some tinkering," Saunders said. "So having one federal standard would be helpful from a compliance standpoint."

Although key congressional leaders have said they're committed to enacting federal privacy legislation, time may be running out, especially as lawmakers begin shifting more of their attention to next year's presidential elections and states keep adding to the patchwork.

"[These state laws] will certainly increase pressure Congress faces from business and lobbying efforts," said Luke Schaetzel, an associate at Benesch Friedlander Coplan & Aronoff. "However, as most states appear to be following a similar mold, the pressure might not be that high if all of the U.S. state laws continue to be very similar."

Additionally, as evidenced by the California delegation's opposition last year to having the American Data Privacy and Protection Act preempt their state's strong privacy protections, Congress is likely to face increased resistance to doing anything more than setting a floor that would allow states to keep establishing higher standards.

"With all these state laws already in place, there's more of a chance that states aren't going to want the federal government to take away their powers and ability to enforce their laws,"
said Melissa Ventrone, leader of the cybersecurity, data protection and privacy business practice at Clark Hill PLC.

These more stringent laws include not only comprehensive privacy frameworks, but also legislation aimed at safeguarding more narrow subsets of data, like information related to children and health care.

California **last year enacted** first-of-its-kind legislation requiring social media platforms to bolster their privacy protections for children, while Washington State last month **enacted** its own groundbreaking law to clamp down on the misuse of wellness, nutrition, fitness, location and other health-related data not covered by the federal law.

The version of the American Data Privacy and Protection Act that passed the House Commerce Committee last summer would override comprehensive state privacy laws while giving states room to enact more targeted consumer protection laws. But federal lawmakers would have to decide if the new wave of narrower, subject-specific privacy laws fit into that exemption, likely further complicating the path to the enactment of a nationwide privacy framework.

Additionally, the fast-moving nature of technology, which includes developments such as the recent explosion in the use of artificial intelligence, could throw a wrench in efforts to set long-lasting federal protections, attorneys say.

"It can be a struggle to get laws on the books that are actually timely and impactful, given how quickly technology changes," said Hutchins of Parker Poe.

The current landscape for privacy legislation resembles the trajectory followed by data breach notification laws, which are currently on the books in all 50 states.

As with consumer privacy laws, California was the first to put a breach notification law on the books in 2003. Now, more than 20 years later, and despite having had numerous chances to set a baseline for reporting cyberattacks, Congress has declined to override state protections, leaving companies to contend with a patchwork.

Unless Congress steps in, the current state law patchwork is likely to continue to spread, bringing with it the potential for not only conflicting rules but also divergent enforcement by state regulators, attorneys say.

"Like the other U.S. states that have enacted data protection laws, [the latest laws] will only act to increase the momentum in other U.S. states," Benesch's Schaetzel said. "They won't want to be left behind as other states take lead on this issue."

Companies also faced a heavy compliance lift when California became the first state to dictate how companies could handle and share consumers' personal information. Virginia complicated those plans by adopting a new model that, among other things, included by-adoption language and data assessment requirements more on par with the European Union's General Data Protection Regulation.

Since then, the framework underlying state privacy laws has remained fairly steady, although variations still abound.

States such as Connecticut and Colorado have instituted tougher rules like enhanced protections for sensitive information and more stringent mechanisms for allowing consumers to opt out of the sharing of their data, while Utah and Iowa left out many such provisions in laws that are widely viewed as being more business-friendly.

The latest batch of laws is no different.

On the heels of Indiana enacting S.B. 5, which will take effect on the first day of 2026, Consumer Reports called on the legislature to strengthen the law during its next session.

The group acknowledged that the Indiana law includes "some basic consumer rights," including the ability to know the information companies have collected about them, the right to delete that information and the right to limit some data disclosures. But it argued that those provisions are "undercut by weak definitions of what constitutes a sale and targeted advertising."

Consumer Reports also criticized the measure for failing to require companies to honor browser signals that allow consumers to opt out of data disclosures on a universal basis; for enabling companies "to discriminate against consumers who exercise their right to opt-out by denying service or charging extra"; and for giving businesses 30 days to cure allege violations flagged by the state's attorney general.

"The Indiana legislature should take a closer look and examine how exactly S.B. 5 protects consumers," said Matt Schwartz, a policy analyst at Consumer Reports. "A closer examination will reveal that there are many loopholes businesses can use to evade the protections considered in this law."

In complying with the Indiana law, companies should pay careful attention to its scope and applicability, Schaetzel said.

While the threshold for being swept up by the law is on par with other states, "if you are a small business operating only in Indiana, but process the personal data of 100,000 or more Indiana consumers, you might be facing new data protection requirements that you've never thought about before," he said.

The law that the Florida legislature passed and sent to the governor's desk on Thursday, on the other hand, takes a different approach to coverage.

Senate Bill 262 defines a "controller" of personal data as having at least $1 billion in global gross revenues — a significant departure from the $25 million threshold found in most other state laws — that either derives 50% of its global gross revenue from the sale of online ads or operates either a consumer smart speaker and voice command service or an app store or digital distribution platform with at least 250,000 different software applications, noted Kyle Dull, a partner at Squire Patton Boggs.

"Based on these threshold requirements, the bill is clearly intended to target only a select group of businesses," Dull said, although he noted that these high thresholds don't apply to businesses that process data on behalf of the large companies that will be covered by the bill and those who receive data in a third-party capacity.

The Florida bill also provides new rights, including the ability for consumers to opt out of the collection of sensitive personal data and the collection of personal data through a voice recognition feature, which will require applicable businesses "to adjust their current consumer rights requests programs to process requests for these new consumer rights" by the time the law takes effect on Dec. 31, 2023, Dull noted.

"Thankfully, the requirements follow the other state laws and mandate such things as specific contractual requirements and an obligation to assist controllers in their compliance with this law," he added.

Consumer Reports has also spoken out against the pending bill in Florida, which in previous sessions fell short of enacting stronger legislation with provisions such as a private right of action.

On Friday, the group called on the state legislature to beef up the "weak" measure, arguing it left "significant loopholes," including its applicability to "only the very largest tech companies" and its failure to extend to most online cookies that fuel targeted advertising, that "would leave Florida consumers' personal information unprotected in a wide variety of contexts."

"This legislation's narrow applicability means that most products and services consumers encounter online, including the vast majority of apps, will not need to follow these new privacy standards," Consumer Report's Schwartz said. "Ad-tech companies will still be able to track users around the internet without their consent. There is a lot of work remaining to ensure the privacy of Florida consumers is truly protected."

The Tennessee Information Protection Act and Montana Consumer Data Privacy Act, which both unanimously cleared their respective legislatures on April 21, are also on the verge of enactment and would add notable wrinkles in companies' compliance plans.

In one of the more unusual provisions of the Montana law, which would take effect in October 2024, the state follows California's lead by requiring companies to obtain consent before selling or using data from users between 13 and 15 years old for targeted advertising.

And the Tennessee law, which companies would have to comply with by July 2025, contains a novel requirement that covered entities implement a data security program that "reasonably conforms to" the privacy framework issued by the federal National Institute of Standards and Technology, giving them an affirmative defense to claims under the new law.

Clark Hill's Ventrone noted that the NIST framework is widely seen as "a good starting point" for security programs and that the requirement in Tennessee to adhere to these standards could help give companies a strong foundation to use in their efforts to respond to privacy laws across the board.

While companies will have time to comply with each new law, attorneys say businesses should take immediate steps to figure out whether they're subject to each measure, take inventory of the data they hold and where it's stored, and decide whether it's time to take a more national — rather than state-by-state — approach to compliance.

"It's getting harder to avoid these laws," Parker Poe's Hutchins said. "If we learned anything from the rollout of GDPR and California's law, it's that companies need to act immediately and be prepared as much as they can, but also leave room to pivot as the rules continue to evolve."

--Editing by Alanna Weissman and Jay Jackson Jr.
