LAW360® Pulse

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

Midyear Review: What GCs Need To Know About Data Privacy

By **Michele Gorman**

Law360 (July 21, 2021, 4:27 PM EDT) -- With the passage of a data privacy measure in Colorado, general counsel during the remaining months of 2021 should understand the privacy laws applicable to their company, consider hiring an in-house privacy specialist, and conduct reassessments on compliance because products and rules evolve.

Earlier this month, Gov. Jared Polis signed into law the Colorado Privacy Act, the third comprehensive consumer privacy legislation in the U.S. The measure, which will take effect in July 2023, requires businesses to give consumers the ability to access, correct, delete and opt out of the sale of their personal information or processing of this data for targeted advertising and profiling purposes.

It has much in common with the privacy laws already on the books in California, Virginia and the European Union, which similarly aim to give consumers more access to and control over how companies handle their personal information. But at the same time, it also introduces **some important nuances** that set it apart from its predecessors, such as establishing heightened protections for the processing of sensitive data and prohibiting the use of "dark patterns" that websites use to trick consumers into making unintended choices.

General counsel will have about two years to comply with most of Colorado's data privacy law, but experts suggest the lawyers use their time wisely and be aware of other emerging measures and trends in the data privacy space.

While some general counsel might think they're set because they've already complied with the EU's groundbreaking General Data Protection Regulation, or GDPR, that **took effect in 2018**, and the landmark **California Consumer Privacy Act** signed into law the same year, privacy is an ongoing build and renovation project because regulations, vendors and products change, said Megan Niedermeyer, vice president of legal and general counsel at data analytics company Fivetran.

"Privacy is not something you do once, and then you're done and you assume that Virginia and Colorado and everything else is just going to follow in the footsteps of the earlier laws that maybe you implemented in-house," she said.

The State Of U.S. Data Privacy Laws

Earlier this month, Colorado's governor signed the third comprehensive privacy piece of legislation in the U.S., and general counsel are now looking at where the consumer privacy law patchwork will expand next.

- Task Force
- Died in Committee or Postponed
-

- No Legislation
- Introduced
- In Committee
- Cross Chamber
- Cross Committee
- Signed into law

Source: International Association of Privacy Professionals
(as of July 21, 2021)

General counsel saw this play out just four months ago with Virginia, where in March the **governor signed** his state's sweeping Consumer Data Protection Act into law. The measure, which is slated to take effect Jan. 1, 2023, departs in several significant respects from its California counterpart, including adopting language and data assessment requirements that are more on par with the GDPR, and leave it completely up to the state attorney general rather than consumers to enforce the law.

This year, Virginia and Colorado both added to the patchwork of state legislation, giving further ammunition to the push for a unified nationwide framework. Vivek Mohan, a partner in Mayer Brown's cybersecurity and data privacy practice, encourages in-house counsel — especially those at companies with a national profile — to take stock of where they are from a privacy, data use and data protection perspective, if they haven't done so already.

"We continue to not see meaningful progress within Congress at a federal level on federal comprehensive privacy legislation," he said. "That means that companies need to spend even more time being attuned to what the real implications of these laws are in the various states, and what the practical steps are to understand, assess exposure and then manage risk."

These laws are emerging as cyberbreaches continue. Federal officials said the recent attack on SolarWinds Corp.'s Orion enterprise network management software **posed a "grave" risk** to businesses. The company's clients include the U.S. Department of Homeland Security, all five branches of the U.S. military, the president's office and Fortune 500 companies.

Another recent high-profile example of a growing threat occurred with the ransomware attack on Colonial Pipeline Co. Hackers caused the country's largest refined petroleum products pipeline system to temporarily halt fuel operations extending from Texas to New Jersey and took down aspects of the company's information technology systems. **Experts said** the attack might make it tougher for companies to negotiate cyber insurance policies without first bolstering their technological defenses.

And in June, McDonald's Corp. joined other U.S. companies when it said it was hit by a data breach, as cyberhackers **gained unauthorized access** to customers' personal data in South Korea and Taiwan.

Data breaches at these big-name companies show all general counsel that any business can be hit at any time, as well as the importance of being prepared, said Suzanne Law Marisa, U.S. general counsel at cloud computing company OVHcloud.

"It's really important to be vigilant about maintaining good cybersecurity practices — having the right administrative protocols in place, all the right policies and procedures, and then implementing the correct technical requirements and companywide training," she said.

For help with tracking and deciphering different state laws, Marisa said her company leans on outside counsel who compile charts that show the scope and requirements of each measure so she can easily distinguish the similarities and differences.

For additional help, she suggested general counsel join the International Association of Privacy Professionals and pay attention to the government's guidance.

For example, the Biden administration in May took a major step toward curtailing the growing scourge of cyberattacks with an **executive order** that imposes heightened cybersecurity requirements on the federal government and its contractors. A month later, the White House **sent an open letter** to businesses warning them to take the risk of ransomware attacks more seriously, while the U.S. Department of Justice issued an internal memo asking prosecutors to prioritize the growing threat.

At the federal level, Mohan warned general counsel to look beyond Congress: The Federal Trade Commission could potentially propose privacy rules, as the agency has taken steps to reduce the administrative burden placed on it under the Magnuson–Moss Warranty Act, which complicated the agency's ability to promulgate regulations under Section 5 of the FTC Act.

While Marisa said she's not overly concerned about being able to comply with Colorado's new law, she recognized that it's one more measure to track — which can be intimidating for any general counsel.

"I'm sure for some folks who really aren't privacy experts, it's really quite overwhelming," she said. "But, again, it's all about having the right advisers in place; it would be hard to do it all by yourself."

And even though it can be daunting, general counsel have months to dig into the recent laws that have been enacted and monitor the measures on the horizon.

"Companies have a decent amount of time — [but] it's not a tremendous amount of time — to understand these frameworks and start to put the implementing building blocks in place so that by the time 2023 comes around, they're well positioned to comply with generally well-thought-out privacy laws that may come into effect in various states," Mohan said.

Niedermeyer said she's keeping a particular watch on Washington state and Illinois because there could be some differences in those measures compared with the laws in California, Virginia and Colorado. Also, they represent major technology hubs and are more entrenched within that ecosystem than other states.

She also mentioned New York, which is further along with its measure and could set the standard for regulation at the state level, which is seen in the financial services sector.

"The more privacy rules, the better," Niedermeyer said. "At some point though, if states diverge from each other, that's where we'll need to see more federal guidance."

About six months into the Biden administration, Niedermeyer said she's hopeful a federal law could see the light of day sooner rather than later.

"I do think there is some unique overlay on both sides of the aisle for caring about not only consumer privacy but best practice privacy as part of the innovation framework for what makes technology companies great," she said. "I hold out a lot of hope over the next four years that as we see more state-by-state legislation … we'll also see deeper entrenchment in wanting to pass the bipartisan federal bill."

--Additional reporting by Allison Grande, Ben Kochman, Shawn Rice and Joyce Hanson. Graphic by Ben Jay.