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

Va. Data Privacy Law Poised To Offer 2nd Model For States

By **Allison Grande**

Law360 (February 12, 2021, 6:39 PM EST) -- Virginia is close to becoming the second state to pass a consumer privacy law that would restrict how companies handle personal information, a development that is set to provide a potentially enticing new model for other states mulling similar moves.

The state's House of Delegates and Senate overwhelmingly approved separate but nearly identical versions of the Consumer Data Protection Act on Jan. 29 and Feb. 3, respectively. Legislators are currently working to reconcile the bills and are widely expected to conclude that process without conflict and send a measure to the governor's desk before their session wraps up at the end of February.

The Virginia proposal, like the landmark California Consumer Privacy Act enacted in June 2018, would establish a host of data privacy rights, including consumers' ability to access, correct, delete and obtain a copy of their personal data from companies and to opt out of the processing of this information for targeted advertising purposes.

But the Virginia law departs in several significant respects from its California counterpart, including by adopting language and data assessment requirements that are more on par with the European Union's General Data Protection Regulation and leaving it completely up to the state attorney general rather than consumers to enforce the law.

"It seems as though we're well on the path toward a patchwork of conflicting state legislation," said Mark Brennan, global lead innovation partner at Hogan Lovells.

Companies have been bracing for the past two years for more states to follow California's lead. But while lawmakers in Washington, New York and a handful of other states have offered promising proposals, they have struggled to pass these measures because of squabbles over how the laws should be enforced and the emergence of the COVID-19 pandemic, which halted most lawmaking efforts.

Virginia's breakthrough is likely to provide both "some encouragement to other states that have seen stumbling blocks" as well as "a potential model going forward" for those that aren't sold on the California framework, according to Kirk Nahra, co-chair of the privacy and cybersecurity group at WilmerHale.

"There are states who would like to have a law but aren't sure where to start," Nahra said. "This

presents an option."

Virginia's entry into the privacy law landscape has been somewhat surprising, given that before the beginning of this year, the state was rarely mentioned in conversations about likely contenders to enact the nation's second comprehensive consumer privacy law.

But, working with one of the shortest legislative sessions in the country, state lawmakers who convened on Jan. 13 have moved quickly to push through privacy protections before they adjourn for the year. The legislative session was originally scheduled to wrap on Feb. 11, but Virginia Gov. Ralph Northam earlier this month called a special session that is slated to run until Feb. 27.

This condensed timeline appears to "have played in favor" for the state by allowing lawmakers to avoid the kind of prolonged debate that has caused similar proposals in other states to fizzle out, said Lydia de la Torre, of counsel at Squire Patton Boggs LLP.

Instead, the Virginia bill focuses on areas where there has generally been broad consensus — such as the need for consumers to be able to access and correct their data — while omitting more controversial provisions, like whether consumers should be allowed to sue for alleged violations.

"This Virginia legislature's decision to bypass the areas where they don't have enough consensus to act and to move on what they do agree on might be a good model for states that want to enact something but aren't able to resolve more complicated questions like whether there should be a private right of action," de la Torre said.

The Virginia proposal combines elements of the California Consumer Privacy Act; the groundbreaking data protection rules that took effect in the EU in 2018; the ballot initiative approved by California voters last year that strengthened the CCPA; and requirements that would be unique to Virginia.

While companies that operate globally are likely to be familiar with these data transparency and access concepts, "the difficulty will be in assessing what rules will apply in what circumstances and making sure that the right notices go out to the right people and the right contracts get updated," said Hogan Lovells partner Bret S. Cohen.

"There are always additional operational realities in putting in place new laws," Cohen added.

Privacy attorneys flagged a host of differences between the proposed Virginia law — which would apply to businesses that handle the personal information of at least 100,000 consumers annually, with a lower threshold of 25,000 consumers for companies that sell data for most of their revenue — and rules that are already on the book elsewhere.

For example, the Virginia measure doesn't restrict how far back consumers can go in asking for a copy of their personal data, meaning companies will have to produce any data they hold about an individual. The CCPA limits data requests to what the company has collected from the consumers during the past 12 months, while the California Privacy Rights Act, the ballot initiative that will replace the CCPA in 2023, will require companies to produce information older than 12 months upon request unless doing so would "involve a disproportionate amount of information or would be unduly burdensome."

Additionally, the proposed Virginia law contains fewer exemptions than the CCPA that companies can leverage to deny consumers' requests to delete their personal information. It also requires companies to

take additional steps to deidentify or pseudonymize personal information so that it's not covered by the law and places more restrictions on what service providers and other third parties that companies share personal data with can do with the information.

Other departures offer helpful clarifications to aspects of the CCPA that have sparked confusion and pushback, said Glenn Brown, a senior member of Squire Patton's data privacy and cybersecurity practice group.

"There are a couple of pretty clear examples of the Virginia legislature trying to learn the lessons that companies had to learn from the CCPA," Brown said.

For example, the Virginia law defines "sale" to mean the exchange of personal data "for monetary considerations," making clear that money must change hands for the law to apply and eliminating the ambiguity that stemmed from the California legislature's decision to define the term to encompass data transfers made for "monetary or other valuable consideration."

The Virginia law would also explicitly exempt loyalty programs from the prohibition on treating consumers differently if they exercise their deletion, correction and opt-out rights under the statute. The nondiscrimination provision in the CCPA didn't include such a carveout, prompting concerns that rewards programs premised on consumers' exchange of information for benefits would need to be discontinued.

The Virginia proposal also notably borrows the GDPR's terminology by referring to those responsible for handling consumer data as controllers and processors — the CCPA calls them businesses and service providers — and by applying to "personal data" rather than "personal information."

"The way that you talk about things matters, and a problem in this space has been that people use terms interchangeably that aren't interchangeable," said Gregory Parks, co-leader of the privacy and cybersecurity practice and retail and e-commerce sector group at Morgan Lewis & Bockius LLP. "So companies will need to figure out if those terms mean the same thing or not, and having to use different language in talking to different subsets of customers will make it harder and more confusing to communicate."

Companies would also be required under the Virginia proposal to undertake data protection assessments in certain circumstances and maintain written agreements with data processors, tasks that are borrowed from the EU law's mandates as well.

Additionally, the Virginia proposal would establish a novel requirement for companies to establish a process for a consumer to appeal if a request to access, delete or correct data is denied. If the appeal is denied, the company would have to provide the consumer with "an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint."

"Providing consumers with a direct path to be connected with the attorney general would mark a fresh approach to potential enforcement in this space," said Brennan of Hogan Lovells.

The state's attorney general, currently Democrat Mark Herring, would be solely responsible for enforcing the Virginia law and could seek damages of up to $7,500 per violation. While the California attorney general is also primarily responsible for enforcing the CCPA, including alleged violations of consumers' data rights, the law does create a limited private right of action that allows consumers to

seek statutory damages of up to $750 per violation for data breaches that result from a company's failure to implement reasonable security procedures.

Also unlike the CCPA, the Virginia proposal doesn't call for the state attorney general to craft regulations on how companies should implement the measure, a process that the California attorney general undertook with significant interest from business, consumer groups and a range of other stakeholders.

On the one hand, implementing the Virginia law without the guidance of attorney general rulemaking is likely to put companies "in a situation where they'll need to take what they consider to be a reasonable position and hope the Virginia attorney general agrees with them, because they won't necessarily know what the attorney general's perspective will be," said de la Torre of Squire Patton.

"It's much more helpful when both consumers and companies know in advance what the rules are that they have to abide by," de la Torre added.

But on the other hand, not having to wait for rulemaking would allow companies to dive right into compliance, rather than having to adjust their efforts each time new draft guidance is released, as many companies found themselves doing in the run-up to the California attorney general's office finalizing its regulations last year, said Kristen Mathews, a partner in the global privacy and data security group at Morrison & Foerster LLP.

"This way, companies would be able to start reading the law and we can start helping clients comply with the law right away," Mathews said.

If enacted as currently drafted, the Virginia law would take effect on Jan. 1, 2023 — the same day that the CPRA and its expanded requirements, including a new right to correction similar to what's in the Virginia proposal, would take effect.

Companies that have already invested in CCPA and GDPR compliance are likely to have a leg up on putting in place the processes and procedures necessary to comply with the new laws. But attorneys say that if the Virginia law is enacted, businesses shouldn't wait to start taking steps such as amending service provider agreements and organizing personal data.

"While there are differences between the two laws, compliance with both the CPRA and this new Virginia law can and probably should be done at the same time over the course of the next two years," Mathews said.

Companies also need to be on the lookout for the emergence of more state privacy laws, and possibly even a federal framework that would unify state requirements.

Washington state has failed for the past two years to push through privacy legislation because of disagreements over whether consumers should be allowed to sue, but the proposal is again receiving serious consideration this year. New York, New Jersey, Oklahoma and Massachusetts are also front-runners to move on consumer privacy protections in 2021.

One of the possibilities in New York, where there are dozens of privacy proposals pending, would set an even higher bar than California or Virginia by allowing consumers to sue for any violations of the law and requiring businesses to act as "data fiduciaries" that are barred from using personal information in a way that benefits them to the detriment of their users.

While attorneys predicted that it may take the enactment of a few more state privacy laws to prompt federal lawmakers to act on long-stalled efforts to implement a national standard, Virginia's quick action is likely to put significant pressure on other states to resolve their differences and join the fray in the coming months.

"If the Virginia law passes, that would likely amp up the work in other states and provide additional motivation for them to work on their own policies," said Hogan Lovells' Cohen. "They don't want to be fourth or fifth or sixth in line, because ultimately the states that come out first are the ones that drive the policies of other states and drive compliance."

--Editing by Alanna Weissman and Jill Coffey.