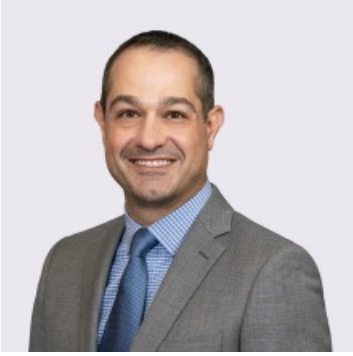
Legal Update Article

Virginia Passes Consumer Privacy Law; Other States May Follow

By Jason C. Gavejian & Joseph J. Lazzarotti

February 17, 2021

Meet the Authors



Jason C. Gavejian
Office Managing Principal
908-795-5139
Jason.Gavejian@jacksonlewis.com

Joseph J. Lazzarotti
Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Related Services

California Advice and Counsel
Privacy, Data and Cybersecurity

When the California Consumer Privacy Act of 2018 (CCPA) became law, it was only a matter of time before other states adopt their own statutes intended to enhance privacy rights and consumer protection for residents. The Virginia legislature has passed such a measure.

On February 3, 2021, the Virginia Senate unanimously passed the Virginia Consumer Data Protection Act (VCDPA), SB1392. The state's House of Delegates had passed the companion bill (HB 2307) in January. Now, legislators are working to reconcile the bills in order to send a measure to the governor's desk before the end of February, when the legislative session concludes.

If signed, the VCDPA will take effect January 1, 2023, the same day as the California Privacy Rights Act (CPRA). The CPRA expands on the protections provided by the CCPA. It was approved by California voters under Proposition 24 in the November election.

Introducing SB1392 in the Virginia Senate, State Senator David Marsden emphasized:

> It is time that we find a meaningful way of protecting the citizens of the Commonwealth of Virginia's data .... Virginia is in a unique position to be a leader on this issue. There's a huge amount of the data on the internet that flows through the commonwealth. Privacy is not a new issue.

Key Elements

Unsurprisingly, VCDPA was modeled on the CCPA, CPRA, and the EU General Data Protection Regulation (GDPR). Key elements of VCDPA include:

- *Jurisdictional Scope.* The VCDPA will apply to businesses that conduct business in Virginia or that produce products or services that are targeted to residents of Virginia and that (i) during a calendar year, control or process data for at least 100,000 Virginian's or (ii) control or process personal data of at least 25,000 Virginia residents and derive over 50 percent of gross revenue from the sale of personal data.
- *Exemptions.* The VCDPA exempts entities subject to HIPAA (both covered entities and business associates), nonprofits, higher education institutions, and financial institutions or data subject to Gramm-Leach-Bliley Act (GLBA). (The HIPAA and GLBA exemptions are more expansive than the CCPA's HIPAA and GLBA exemptions, which provide only an exemption for data subject to the HIPAA and GLBA.)
- *Personal Data.* Similar to the CCPA and GDPR, the VCDPA defines personal data broadly to include "any information that is linked or reasonably linkable to an identified or identifiable natural person."

- *Sensitive Data.* Like both the GDPR and the CPRA, the VCDPA includes a category for "sensitive data." This is defined as "personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; … [t]he processing of genetic or biometric data for the purpose of uniquely identifying a natural person; … [t]he personal data collected from a known child; or … [p]recise geolocation data." There are two key compliance obligations related to sensitive data. First, sensitive data cannot be processed without consumer consent. Second, the controller must conduct and document a data protection assessment specifically for the processing of sensitive data.
- *Consumer.* The VCDPA defines "consumer" as "a natural person who is a resident of the Commonwealth acting only in an individual or household context." The VCDPA states that the definition of consumer *does not* include a "natural person acting in a commercial or employment context."
- *Consumer Rights.* Under the VCDPA, Virginia residents will be afforded the following personal data rights:
    - To confirm whether or not a controller is processing their personal data and to access such personal data;
    - To correct inaccuracies in their personal data, taking into account the nature of the personal data and the purposes of the processing of their personal data;
    - To delete personal data provided by or obtained about them;
    - To obtain a copy of their personal data that they previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows them to transmit the data to another controller without hindrance, where the processing is carried out by automated means; and
    - To opt out of the processing of the personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning them.
- *Data Protection Assessments.* The VCDPA imposes a new requirement for controllers: data protection assessment obligations (as mentioned above regarding sensitive data). Controllers must conduct data protection assessments for specific processing activities involving personal data. These activities include targeted advertising, sale of personal data, profiling, sensitive data, and data that presents a heightened risk of harm to consumers.
- *Enforcement.* The Virginia Attorney General's office would have exclusive enforcement over the VCDPA. In addition, a controller or processor must be provided 30 days' written notice of any violation, allowing the entity the opportunity to cure the violation. Failure to cure the violation could result in a fine of $7,500 per violation. A private right of action is not available.

Other State Consumer Privacy Legislative Activity

Virginia may be the first state to follow California's lead on consumer privacy legislation, but it certainly will not be the last. The International Association of Privacy Professionals (IAPP) observed, "State-Level momentum for comprehensive privacy bills is at an all-time high." The IAPP maintains a map of state consumer privacy legislative activity, with in-depth analysis comparing key provisions.

A few other state bills to watch in 2021:

- *Florida HB 969 (HB569)* – On February 15, Governor Ron DeSantis announced a

data privacy bill similar to the CCPA. In particular, the bill would require certain businesses to provide notice to consumers about data collection and selling practices and provide consumers the right to request that certain data be disclosed, deleted, or corrected and to opt-in or opt-out of sale or sharing of such data. A private cause of action is available under the bill. If passed, the bill will become effective January 1, 2022.

- *Minnesota HF 36 (HF36)* – Introduced in the Minnesota state legislature, and similar to other state proposals, HF36 would provide consumers various rights regarding their personal data and place data transparency obligations on covered businesses. The bill would create a private right of action with statutory damages, ranging from $100 to $750 per consumer and per incident, and provide for enforcement by the attorney general.
- *New York Privacy Act 2021 (NYPA) (A680)* – The NYPA had beenintroduced in a previous legislative session, but failed to move forward in the legislative process. The NYPA is considered a more expansive version of the CCPA. For example, unlike the CCPA's threshold for covered businesses of $25 million in annual revenue, the NYPA would apply broadly to "legal entities that conduct business in New York" or businesses that "intentionally target" New York residents. The bill also includes a strict consent requirement like the GDPR, which is "for all processing activities and third-party disclosures, with no exceptions."
- *New York Senate Bill S567 (S567)* – A second bill moving through New York's legislative process is S567, which mirrors the CCPA almost entirely. A key distinction between S567 and the CCPA, however, is S567's private right of action. S567 provides a private right of action for consumers who have suffered an injury and "any person who becomes aware, based on non-public information, that a person or business has violated this section may file a civil action for civil penalties." In theory, therefore, suits could be brought by vendors, competitors, or even consumer privacy policy groups.
- *Oklahoma "An Act Relating to Data Transparency" (HB1130)* – Similar to laws passed by Maine and Nevada in 2019, Oklahoma's HB1130 would impose data transparency obligations on online businesses or websites that include conspicuously posting on its website homepage in a plain readable format as to the categories of personal information to be collected and the purposes for which the categories of personal information will be used. In addition, the bill would prohibit covered entities from collecting or using additional categories of personal information without providing the consumer an updated compliant notice.
- *Washington Privacy Act 2021 (WPA) (SB 5052)* – For three consecutive years, the Washington state legislature has introduced versions of the WPA. In 2019, the bill failed in the Assembly. In 2020, the Assembly passed an amended version of the bill, but the two chambers failed to reach a compromise regarding enforcement provisions. Currently in committee, the WPA would impose GDPR-like requirements on businesses that collect personal information related to Washington residents. In addition to requirements for notice and consumer rights such as access, deletion, and rectification, the WPA would impose restrictions on use of automatic profiling and facial recognition.

Although more limited in scope than CCPA-like, these proposals show how complicated the patchwork of laws will become as more states enact their own privacy laws with inconsistent with each other and often include mutually exclusive requirements.

Takeaway

States across the country are contemplating ways to enhance their data privacy and security protections. Organizations, regardless of their location, should be assessing and reviewing their data collection activities, building robust data protection programs, and investing in written information security programs.

Please contact a Jackson Lewis attorney with any questions.