Two's Company: Virginia Has a Comprehensive Data Privacy Law

Aaron J. Burstein, Alysa Z. Hutnik

March 3, 2021

On March 2, Governor Ralph Northam signed the Virginia Consumer Data Protection Act (VCDPA) into law, making Virginia the second state to enact comprehensive privacy legislation.

With the VCDPA on the books, companies have the next 22 months to prepare for the VCDPA and the California Privacy Rights Act (CPRA) to go into effect. This post takes a look at the VCDPA provisions that are novel and require close attention during the transition period to the law's January 1, 2023 effective date.

- **Sensitive Data:** The VCDPA breaks new ground in U.S. privacy law by requiring consent to process "sensitive data" – a term that includes precise geolocation data; genetic or biometric data used to identify a person; and data revealing race or ethnicity, religious beliefs, health diagnosis, sexual orientation, or citizenship or immigration status. The definition of "consent," in turn, tracks the GDPR definition: "freely given, specific, informed, and unambiguous" and conveyed by a "clear affirmative act."

- **Opt-Outs:** Controllers will need to offer opt-outs under three distinct circumstances. In addition to an opt-out of sale (which is limited to exchanging personal data for monetary consideration), controllers must allow consumers to opt out of (1) "targeted advertising" and (2) "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." Although the definition of "targeted advertising" excludes ads "based on activities within a controller's own websites or online applications" (which also appears to include affiliates' websites), it is unclear whether this exclusion encompasses, for example, a controller's use of third-party data sources combined with its first party data to inform its targeting decisions. As a result, VCDPA opt-outs could have a significant impact on first-party data use as well as third-party data sharing. Notably though, the law clearly excludes from the targeted advertising definition the processing of personal data solely for measuring or reporting advertising performance, reach, or frequency.

- **Principles for Data Controllers:** Section 59.1-574 articulates several broad, principles-based obligations of data controllers, including reasonable security and a duty to limit personal data collection to what is "adequate, relevant, and reasonably necessary" to fulfill purposes that have been disclosed to consumers. Companies have gained experience with similar principles under the GDPR and federal and state reasonable security requirements, but their inclusion in comprehensive privacy legislation that provides civil penalties of up to $7,500 per violation counsels in favor of taking a close look at how to demonstrate a thoughtful, well-reasoned approach to data strategies.

- **Data Protection Assessments:** Controllers will need to conduct data protection assessments not only for high-risk activities but also for targeted advertising, profiling, personal data sales, and sensitive personal data processing. These assessments will be fair game for the Attorney General in any investigation of a controller's compliance with the data protection principles and transparency requirements of section 59.1-574, though the VCDPA purports to preserve attorney-client privilege and work product protection for assessments submitted in response to a civil investigative demand. The affirmative obligation to conduct such assessments does not begin until January 2023.

- **In and Out of Scope:** The Virginia law focuses on Virginia residents in their capacity as a consumer, and expressly excludes a person acting in an employment or commercial (B2B) capacity. The law also excludes GLBA-covered financial institutions and financial personal information, FCRA-covered information, HIPAA covered entities and their business associates, non-profits, and higher education. Publicly-available information is also outside the scope of regulated personal information, and extends to data from publicly-available government records or when lawfully made available to the general public.

- **No Private Right of Action:** The Virginia law provides the Attorney General with the exclusive authority to enforce the law and that it should not be used as a basis to bring a private suit under the act or any other law. However, as we've seen with the CCPA, that type of restriction has not stopped parties from pursuing creative ways to bring private actions for privacy violations, including under other provisions of state law, such as unfair and deceptive trade practice statutes.

For better or worse, companies will need to prepare for the VCDPA without an obvious prospect of additional regulatory guidance. Unlike the regulatory structure the CCPA established – and the CPRA significantly expands, Virginia's privacy law does not provide any state agency or official with rulemaking authority. However, the VCDPA could be just a first step. Governor Northam reportedly "will have an ongoing work group to continue to strengthen the law's consumer protections," and Virginia Delegate Cliff Hayes, who introduced the House version of the law, signaled that legislators are open to making such changes. It will remain to be seen the extent to which this group will recommend allocating additional funding to the Attorney General's office to enforce the law, and the type of enforcement we may see. Historically, the office has not been as active as other state attorneys general on consumer protection related matters outside of a fraud context.

We will watch closely for changes in Virginia and progress in other state privacy bills.