Analysis

Virginia, Not California, Is Privacy's Next Top Model

Mark E. Smith
CIPP/US, CIPP/C, CIPM
Bloomberg Law Legal Analyst

Bloomberg Law

Virginia, Not California, Is Privacy's Next Top Model

By Mark E. Smith, CIPP/US, CIPP/C, CIPM, Bloomberg Law Legal Analyst

The future of consumer privacy now has a sleek East Coast vibe with Virginia's enactment of the Consumer Data Protection Act (VCDPA). A mere eight pages long, Virginia's take on consumer privacy contrasts sharply with the extensive, highly detailed obligations draping the California Consumer Privacy Act (CCPA). And with additional requirements woven into the lengthier California Privacy Rights Act (CPRA), Virginia's slim cut is undoubtedly a better fit for business.

Entering into effect Jan. 1, 2023, the VCDPA introduces a tailored approach to comprehensive (i.e., non-sectoral) privacy legislation. Far from being a CCPA imitation, the Virginia law is a no-nonsense act, covering what's necessary without excessive embellishment. In the absence of federal legislation, I see businesses willing to embrace the Virginia model for a number of reasons.

Clean Lines

First, the statute is written so that businesses can readily identify what's covered and who must comply.

The VCDPA defines "personal data" as "any information that is linked or reasonably linkable to an identified or identifiable natural person." That's a far cry from California's definition of "personal information," which "includes, but is not limited to," a laundry list of identifiers, categories, characteristics, data sets, and inferences that are "reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."

The VCDPA mentions no households. No potential associations. No indirect connections. And (fortunately) no exhausting while non-exhaustive list of examples. As such, businesses needn't speculate about information that might possibly be covered by the statute. As long as the information is "linked or reasonably linkable," it's within scope.

Moreover, the VCDPA clearly defines whose personal data is covered. It describes consumers as Virginia residents "acting only in an individual or household context." It further clarifies that consumers are not those acting in a "commercial or employment context." Thus, unlike California, where the B2B and employee exclusions have been the subject of several statutory amendments and are still set to expire in 2023, Virginia has chosen not to leave those potential compliance hurdles up in the air.

A definite boon for business!

Entities conducting business in Virginia must satisfy one of two thresholds to fall within the statute's scope, and both thresholds address a minimum number of affected consumers. Entities must control or process (i) the personal data of at least 100,000 consumers in a calendar year, or (ii) the personal data of at least 25,000 consumers, while deriving over 50 percent of gross revenue from the sale of that data.

Unlike California, the VCDPA makes no mention of a threshold based solely on annual gross revenue, so entities are not left to question whether the processing of data from a dozen or so consumers will subject them to the law.

Moreover, VCDPA clearly identifies those falling *outside* the scope of the law, including state agencies, nonprofit organizations, colleges and universities, financial institutions covered by the Gramm-Leach-Bliley Act, and covered entities or business associates governed by HIPAA and its implementing regulations.

European Flair

While simplicity relative to California's setup contributes to much of the VCDPA's appeal, tasteful incorporation of certain features from the European Union's General Data Protection Regulation (GDPR) gives it both practicality and sophistication.

Privacy professionals both inside and outside Europe recognize the GDPR as the de facto standard for consumer privacy legislation. Accordingly, the VCDPA borrows a number of terms from the GDPR—"controller," processor," "personal data"—thereby giving a bit of comfort and familiarity to businesses already handling GDPR compliance. And its assimilation of GDPR principles such as data minimization and transparency is simply a matter of good policy, for businesses and consumers alike.

Still, the VCDPA is essentially an opt-out regime. It generally permits businesses to process personal data, provided they inform consumers of what's being processed and why. While it does require GDPR-esque consent in certain situations—before processing sensitive data, and before processing any personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes—the restrictions are minimal, and should already align with standard business practices.

Versatile Design

It goes without saying that the VCDPA benefits consumers, too, for it recognizes key consumer rights: the right to know what personal data is being processed; the right to access, correct, and delete that data; the right to data portability; and the right to opt out of the sale of personal data or the processing of personal data for targeted advertising or profiling.

The VCDPA also protects consumers by requiring businesses to "establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data."

Beyond data security practices, the VCDPA requires businesses to conduct a data protection assessment for certain activities. While at first that may seem like an undue burden on business, the assessment is a sensible, risk-based analysis, weighing the benefits of processing against the potential risks to the rights of the consumer. Since businesses may take into account any safeguards used to mitigate such risks, the statute is merely emphasizing good business practices that should already be in place.

Of course, the VCDPA requires businesses to provide consumers with a "reasonably accessible, clear, and meaningful privacy notice," but the statute is not overly prescriptive, so businesses have a great deal of leeway regarding how to convey the information. Unlike California, the VCDPA does not require the placement of "do not sell" links, nor does it mandate special notices at collection.

Ready to Wear

Aside from documenting data protection assessments, Virginia's law has no significant recordkeeping requirements. And if a business already has in place a GDPR- or CCPA-compliant process for receiving and responding to data subject or consumer access requests, that process should be sufficient to handle requests from Virginia residents. The only potential alteration for Virginia requests would involve cases where a request is denied. The VCDPA requires controllers to notify consumers of the basis for the denial and instructions for how to "appeal" that decision.

The appeal process itself appears to be an internal review—i.e., the controller reviews the initial denial and informs the consumer "in writing of any action taken or not taken in response to the appeal." If the appeal is denied, the controller must 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."

And speaking of the attorney general, the VCDPA provides exclusive enforcement authority to the AG. There's no overarching Supervisory Authority, as with the GDPR. No creation of a privacy protection agency, as with the CPRA. And thankfully (for business), no private cause of action.

Accessory-Free

If the features mentioned above are not enough to win over businesses, the VCDPA ties an extra bow on top: It does not direct the attorney general's office to draft implementing regulations.

Given that the California AG has just adopted the *fourth* set of modifications to the CCPA's regulations, the Virginia model has come into vogue almost overnight.

For more Bloomberg Law Analysis, visit https://news.bloomberglaw.com/bloomberg-law-analysis/.