American Bar Association, Section of Litigation
Privacy and Data Security Committee

ARTICLES

Virginia Set to Become the Second State to Enact Holistic Data Privacy Law

The act purports to regulate the collection, use, and disclosure of the personal data of Virginia's residents generally.

By Glenn A. Brown – February 25, 2021

In the coming days, Governor Ralph Northam is expected to sign into law the Virginia Consumer Data Protection Act, which, if enacted, will become effective on January 1, 2023. As a result, Virginia would become the second state in the United States to enact a holistic data privacy law that purports to regulate the collection, use, and disclosure of the personal data of its residents generally.

Overview and Quick Take

In many ways, the act is similar to the California Consumer Privacy Act (CCPA), the first holistic data privacy law in the U.S., and to the California Privacy Rights Act (CPRA), which was enacted by ballot referendum in November 2020. It also shares some concepts with the European Union's General Data Protection Regulation (GDPR). However, it is sufficiently dissimilar to each of those laws that a business developing a compliance strategy for the act will not be able to rely solely on its previous compliance efforts in complying with the act.

It is clear that in drafting the act, Virginia legislators wanted to avoid some of the ambiguous provisions of the CCPA and CPRA. For instance, the act defines the sale of personal data as occurring only when monetary consideration is exchanged for personal data, which makes the analysis of when a "sale" occurs a lot simpler than under the CCPA or CPRA, which considers a sale to occur when the exchange of personal information is for "money *or other valuable consideration*."

However, the instances in which the act is clearer than the CCPA and CPRA are more than offset by the lack of detail regarding many of its key requirements. As an example, the act provides consumers with a right to access their personal data held by a controller. Similarly, the CCPA requires a business to provide a consumer with his or her personal information that the business has collected during the previous 12 months. The CPRA allows consumers to request the disclosure of personal information collected more than 12 months prior to the request, but a business only has to disclose personal information collected after January 1, 2022. The act provides for no limitations on the "look-back" period, which effectively puts the onus on controllers to weigh the benefits of continuing to retain aging personal data against the burdens of having to produce such personal data upon request.

We discuss below the key provisions of the act and note where they differ from requirements under similar laws, such as the CCPA and CPRA. It is unclear whether any clarifying regulations or rules will be promulgated in connection with the act.

Key Terms

Before discussing the act's substantive requirements, it is helpful to understand how the act defines key terms and how such definitions compare with those of other privacy laws.

Consumer

The act defines a "consumer" as a natural person who is a resident of Virginia. Crucially, it specifies that a Virginia resident is a "consumer" only when acting in an individual or household context, and it expressly does not include a natural person acting in a commercial or employment context. By contrast, the CPRA will apply to consumers, even when they are acting in a commercial or employment context. The GDPR similarly applies to individuals more broadly.

Controller and Processor

These definitions track the definitions in the GDPR, with the former being defined as a natural or legal person that, alone or jointly with others, determines the purpose and means of processing personal data, and the latter being defined as a natural or legal person that processes personal data on behalf of a controller. These terms are similar but not identical to the terms "business" and "service provider" in the CCPA and CPRA.

Personal Data

The act defines "personal data" as any information that is linked or reasonably linkable to an identified or identifiable natural person. "Personal data" does not include de-identified data or publicly available information, as those terms are defined. This is similar to definitions in other privacy laws, although the act does not provide a list of specific categories of personal data, as the CCPA and CPRA do in their definitions of "personal information."

Sale of Personal Data

The act defines a "sale of personal data" as an exchange of personal data for monetary consideration by the controller to a third party. As mentioned above, this is a significant departure from the definition of "sale" in the CCPA and CPRA. By expressly requiring *monetary* consideration to be exchanged for personal data in order for a sale to exist, the act allows a business to transfer personal data for many activities that are the focus of regulatory attention elsewhere (such as targeted advertising) without having to characterize such transfers as sales. Note that transfers of personal data to affiliates and to third parties in certain types of transactions are excluded from the definition of "sale of personal data" under the act.

Sensitive Data

The act defines "sensitive data" as personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; genetic or biometric data (if processed for the purpose of uniquely identifying a natural person); the personal information of a known child; and precise geolocation data (as defined in

the act). The similar term found in the CPRA, "sensitive personal information," is significantly broader; it includes such information as Social Security numbers, driver's license numbers, credit or debit card numbers, and the content of communications (unless the business is the intended recipient).

Applicability of the Act

The act provides rights to natural persons who are Virginia residents and generally imposes obligations on any natural or legal person that

- conducts business in Virginia or produces products or services that are targeted to Virginia residents; and
- in a calendar year, either
- controls or processes the personal data of at least 100,000 Virginia residents; or
- controls or processes the personal data of at least 25,000 Virginia residents *and* derives at least 50 percent of its gross revenue from the sale of personal data.

Unlike the CCPA and CPRA, the act does not include a revenue component for determining applicability; instead, the act focuses on the number of consumers whose personal data are controlled or processed. Therefore, even very large businesses doing business in Virginia will not be subject to the act if they do not meet one of two volume-based thresholds described above. Another difference is that under the CCPA, the only condition on applicability for "service providers" (the equivalent of a processor under the act) is that they be for-profit organizations, while the act's applicability thresholds apply to controllers and processors alike.

There are also some significant exclusions. The act provides that it does not apply to, among other things,

- any Virginia state or local government agency or body and institutions of higher learning, as defined;
- financial institutions subject to the Gramm-Leach-Bliley Act (GLBA);
- information regulated by any of the GLBA, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Farm Credit Act, and the Family Educational Rights and Privacy Act;
- covered entities and business associates, as those terms are defined by the Health Insurance Portability and Accountability Act (HIPAA);
- certain types of nonprofit organizations (corporations organized under the Virginia Nonstock Corporation Act and organizations exempt from taxation under sections 501(c)(3), 501(c)(6), and 501(c)(12) of the Internal Revenue Code); and
- protected health information, as defined under HIPAA, and certain other types of health-related information.

Note that unlike the CCPA and CPRA, the act provides for entity-level exemptions. This means that a financial institution subject to the GLBA or a covered entity or business associate under

HIPAA would be exempt from complying with the act, even if it holds personal data that are not specifically exempt under the act.

Rights of Consumers

The act provides Virginia residents with the following rights:

Right to Access

The act provides consumers with a right to know whether a controller processes the consumer's personal data and to access such data. As mentioned above, the act does not limit the scope of personal data that a controller is required to provide to the requesting consumer. The act provides for no exceptions and applies to all personal data subject to the act, whenever collected.

Right to Correct

The act provides consumers with a right to correct inaccuracies in the consumer's personal data. However, unlike the CPRA, which does not require a business to use disproportionate efforts in responding to a request and acknowledges that a business must have methods to prevent fraud in order to fulfill such requests, the act does not provide any exceptions or acknowledge competing considerations in responding to requests to exercise this right.

Right to Delete

The act provides consumers with a right to request that a controller delete all personal data collected about the consumer from any source. This and other aspects of the act are subject to a controller's and impacted parties' exercise of their First Amendment rights, however.

Right to Opt Out

The act provides consumers with a right to opt out of the processing of personal data for the following purposes:

- targeted advertising (defined to include displaying advertisements that are selected based on personal data obtained from that consumer's activities over time and across unaffiliated websites to predict the consumer's preferences or interests, but subject to several exceptions);
- the sale of personal data; or
- "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer," as that phrase is defined.

The right to opt out of processing for this last purpose is interesting: It allows a consumer to opt out of a controller's use of automated processing to make a decision "that results in the provision or denial by the controller of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, such as food and water."

However, using personal data to make decisions about lending, housing, insurance underwriting, or employment is generally regulated by the Fair Credit Reporting Act and, so in most cases,

should be exempt from the act. This could create confusion for consumers and headaches for controllers that engage in these types of processing activities.

Right to Appeal Decisions
The act gives consumers the right to appeal a controller's refusal of a request. Within 60 days of receiving an appeal, a controller must inform the consumer in writing of its response to the appeal, including a written explanation of the reasons for the decision. If the controller denies the appeal, it must also provide the consumer with an online mechanism (if available) or other method through which the consumer can submit a complaint to the attorney general.

Like the CCPA and CPRA, the act provides that controllers must respond to rights requests within 45 days, which period the controller may extend once for an additional 45-day period if it provides notice to the requesting consumer explaining the reason for the delay. Controllers may charge reasonable administrative fees or deny a consumer's request if the request is manifestly unfounded, excessive, or repetitive.

Obligations of Controllers

In addition to providing consumers with the rights described above, the act imposes certain obligations on controllers, including the following:

Data Minimization
The act provides that controllers must limit the collection of personal data to that which is "adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed." The CPRA and GDPR also impose a similar data minimization obligation.

Limitations on Use
The act provides that unless a controller obtains a consumer's consent, it must not process personal data for purposes that are neither reasonably necessary to, nor compatible with, the purposes that the controller has disclosed to the consumer. The act also requires controllers to obtain a consumer's consent in order to process sensitive data (as defined). Although this a more burdensome obligation than the obligations imposed on "sensitive personal information" under the CPRA, the act's definition of "sensitive data" is significantly more limited.

Reasonable Data Security
The act requires controllers to establish and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data maintained by the controller. The GDPR and CPRA have similar requirements.

Data Protection Assessments
The act requires controllers to undertake data protection assessments of certain types of processing activities created or generated after January 1, 2023. The act specifies the matters such assessments must address. However, the act does not specify how often controllers are required to conduct these assessments or for how long they must be retained. Upon request and

to the extent relevant to an investigation, a controller must provide copies of such assessments to the attorney general (who is responsible for enforcing the act).

Contracts with Processors
The act requires that a controller's contract with a processor clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties. The act also includes specific terms that must be included in such contracts relating to the processor's use and disclosure of personal data. An odd result of the act's inclusion of applicability thresholds for processors is that a controller would not seem to be required to include any of these terms in contracts with small vendors that do not meet the thresholds described above under the heading Applicability of the Act.

Antidiscrimination
The act prohibits controllers from processing personal data in violation of antidiscrimination laws and from discriminating against consumers for exercising their rights under the act. However, the act avoids some of the interpretational challenges created by the CCPA's antidiscrimination prohibition and requirements for offering "financial incentives" in the context of typical loyalty and rewards programs offered by retailers. The act clearly provides that it does not prohibit a controller from providing a different price, rate, level, quality, or selection of goods or services to a consumer if the offer is "related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program."

Privacy Notice
Similar to other privacy laws, the act requires controllers to provide a privacy notice to consumers that includes certain specified disclosures, but unlike those other statutes, the act does not address when the controller must provide the notice or the means of delivery.

Obligations of Processors
Compared with controllers, processors have relatively few obligations under the act. The following are their primary obligations:

Following the Instructions of the Controller
The act requires processors to adhere to the instructions of a controller and to assist it in the matters described below.

Assistance to Controllers
Processors must assist controllers with responding to consumers' rights requests, with meeting the controller's obligations relating to the security of personal data and giving notice of a security breach, and with the processor's creation of the data protection assessments described above.

Enforcement and Liability

There is no private right of action for violations of the act; the Virginia attorney general has exclusive enforcement authority. The attorney general may seek injunctive relief and civil penalties of $7,500 per violation. However, as required by the CCPA (but not the CPRA), the attorney general must provide a controller or processor with 30 days' written notice of any violation of the act, specifying the provisions that the attorney general alleges have been violated. A controller or processor can avoid statutory damages if, within this 30-day cure period, it cures the noticed violation and provides the attorney general an express written statement that the alleged violations have been cured and that no further violations will occur.

The act provides that a controller or processor that complies with the act in disclosing personal data does not violate the act if the third party, controller, or processor that receives such personal data violates the act (assuming the disclosing party had no actual knowledge that the recipient intended to violate the act). Likewise, a third party, controller, or processor receiving personal data does not violate the act due to the disclosing party's violations of the act.

Conclusion

In light of the differences between the act and existing privacy laws, businesses will need to consider carefully the varying obligations under each of these laws and the potential exposure based on the nature of their business and the types of personal data they process. Businesses should then thoughtfully design a defensible compliance strategy that minimizes the operational impact to the business. Assessing these issues under the act will be challenging, given the lack of detail surrounding many of the act's provisions and the lack of clarity as to whether any supplementing regulations or rules will be forthcoming.

The privacy laws in California and Virginia are the continuation of a trend expected to result in new privacy legislation in Washington, Oklahoma, New York, and elsewhere in the near future. Companies operating in the U.S. will need thoughtful privacy compliance strategies based on defensible interpretations of these laws, a good understanding of where they overlap and where they differ, and an assessment of the relevant regulatory, reputational, and enforcement risks.

Glenn A. Brown is of counsel with Squire Patton Boggs in Atlanta, Georgia.