The Computer & Internet Lawyer

Volume 38 ▲ Number 7 ▲ July/August 2021

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

What Virginia's New Consumer Data Protection Act Means for You and Your Data Collection

By Jeffrey M. Mann

Earlier this year, the state of Virginia enacted the Consumer Data Protection Act ("CDPA"), which includes wide ranging privacy regulations. While the CDPA is not the first legislation of its kind in the United States and is similar to other privacy regulations throughout the world, it has its own nuances and is a clear indication that in the absence of a uniform federal privacy construct from Congress, states will be moving forward to pass their own regulations. In fact, numerous other states have pending bills in the legislature currently related to privacy protections for consumers. At the time of the writing of this article, Colorado appeared to be on the verge of becoming the third state to enact its own comprehensive data privacy legislation with the passing of the Colorado Privacy Act on June 7, 2021.

Jeffrey M. Mann, a Special Counsel in the Intellectual Property and Technology Group at Stroock & Stroock & Lavan LLP, is a registered patent attorney and certified information privacy professional ("CIPP/US"). Mr. Mann focuses his practice on all facets of intellectual property and technology, including transactional work, licensing, opinion work, patent prosecution, cybersecurity, and privacy. He may be contacted at *jmann@stroock.com*.

The CDPA does not go into effect until January 1, 2023, but it is never too early to make sure that your data policies and practices are updated.

Applicability

The CDPA is applicable to any individuals or entities that "conduct business in the Commonwealth [of Virginia] or produce products or services that are targeted to residents of the Commonwealth" and that:

- During a calendar year control or process the personal data of at least 100,000 consumers; or
- Control or process personal data of at least 25,000 consumers and derive at least 50 percent of gross revenue from the sale of personal data.

Unlike the existing California Consumer Privacy Act ("CCPA") or the California Privacy Rights Act ("CPRA"), which is slated go into full effect in 2023, Virginia's CDPA does not have an independent revenue threshold. Therefore, under the CDPA even large revenue generating companies will not be subject to the regulations if they do not meet the minimum personal

data requirements set forth above. This will reduce the number of companies that are potentially subject to the new privacy requirements under the CDPA.

Consumer Rights

Similar to the General Data Protection Regulation ("GDPR") in Europe, the CDPA uses the concept of a "Controller" to refer to the entity or individual that determines the purpose and means of data processing and a "Processor" to refer to the entity or individual that actually carries out the processing of data on behalf of the Controller.

The CDPA provides individuals who reside in Virginia ("Consumers") with five primary rights:

1. *Right to Access Your Data*. Consumers are entitled to "confirm whether or not a controller is processing the consumer's personal data and to access such personal data."

2. *Right to Correct Your Data*. Consumers are entitled to have any inaccuracies in their data corrected taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

3. *Right to Delete Your Data*. Consumers are entitled to request that their personal data be deleted by the Controller.

4. *Right to Obtain Your Data*. Consumers are entitled to obtain a portable copy of their personal data previously provided to the Controller and, to the extent technically feasible, in a format that allows the consumer to transmit the data to another Controller without hindrance, where the processing is carried out by automated means.

5. *Right to Opt Out*. Consumers are also entitled to opt out of the processing of the personal data for purposes of "targeted advertising, the sale of personal data, or profiling."

Under the CDPA these rights are absolute and the Controller must comply without undue delay, but in all cases within 45 days. This 45-day period may be extended for one additional 45-day period, if reasonably necessary.

If a Controller declines to take action or is unable to authenticate the request, the Controller must provide the consumer with an appeal process to appeal the refusal to comply with the request and include a written explanation for their decision. If the appeal is denied, the Controller must provide the Consumer with an online mechanism, or if not available, another method for the Consumer to submit a complaint to the attorney general.

Over the coming months it will be interesting to see if any additional guidance or exceptions regarding individual circumstances that may prevent a Controller from complying with a Consumer request will be forthcoming.

Data Not Covered Under the CDPA

The CDPA only covers data that is linkable to an identified natural person, but not data that would only identify a household. This differs from the CCPA definition of personal information which also includes information that could reasonably be linked to a household.

It is also noteworthy that the CDPA does not apply to employee data. This will make compliance less onerous on entities that have had difficulties in complying with employee provisions in the CCPA and other privacy laws. The CDPA also does not apply to nonprofit organizations or institutions of higher education.

Additionally, the following organizations and data are also excluded from compliance with the requirements of the CDPA:

- Financial institutions or data subject to Title V of the federal Gramm-Leach-Bliley Act;

- Any covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164 established pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA");

- Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994; and

- Personal data regulated by the federal Family Educational Rights and Privacy Act ("FERPA").

Cybersecurity and Data Protection Requirements

An additional unique aspect of the CDPA is that it also creates cybersecurity and data protection requirements that are not in other existing privacy regulations. For example, the CDPA requires that businesses maintain "reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data."

The security practices are required to be "appropriate to the volume and nature of the personal data at issue." There is no specificity in the CDPA as to what reasonable practices would be and time will tell how strictly these requirements will be enforced by the attorney general.

Controllers are also required to conduct and document data protection assessments. These assessments are required to cover any processing activities that include targeted advertising, the processing of sensitive data, the sale of personal data, or the processing of personal data for the purposes of profiling. The activities related to profiling are only where such profiling presents "a reasonably foreseeable risk" of:

- Unfair or deceptive treatment of, or unlawful disparate impact on consumers;
- Financial, physical, or reputational injury to consumers;
- A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or
- Other substantial injury to consumers.

Right of Enforcement

Lastly, one other major difference between the CDPA and other privacy regulations is that the CDPA does not allow for a private right of action, but rather the attorney general has the sole right of enforcement. This may limit the amount of litigation or other legal action that results from the CDPA.

The attorney general does have the right to seek an injunction to restrain any violations of the CDPA and assess up to $7,500 for each violation.

Conclusion

The CDPA is the newest of the privacy regulations and has much in common with other privacy laws. However, while the CDPA has much in common with other privacy regulations, it is clear that compliance with the other paradigms may not suffice to be fully compliant with the CDPA.

Accordingly, companies and privacy professionals will have to carefully consider the applicability of the CDPA and take the necessary steps to make sure they are compliant with all of its new and slightly altered privacy requirements.