Articles + Publications | March 8, 2021

Privacy Laws Begin to Ripple Across the States Following the California Consumer Privacy Act

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos

As we have discussed in previous articles, through the California Consumer Privacy Act (CCPA), California has set new privacy standards, granted new consumer rights, and imposed new obligations on businesses. Although clearly inspired by the EU's General Data Protection Regulation, the CCPA introduced novel concepts for privacy laws in the U.S. With the enactment of the Virginia Consumer Data Protection Act as signed by the governor on March 2, 2021, it is clear that California has inspired change to the privacy landscape across the U.S. Four more states, also inspired by the CCPA, have introduced privacy bills, at least some of which are expected to pass in 2021.

We have seen this movie before. In 2002, California adopted the first state data breach notification requirement. These laws rippled across the U.S., and by 2018, all U.S. jurisdictions had a breach notification requirement similar in key respects to California's prototype.

After enactment of the CCPA in 2018, it appeared that a bill in Washington State (SB 6281), comparable in many ways to the CCPA, would follow almost immediately. The Washington bill was abandoned, however, and no other state enacted a sweeping privacy law. Bills essentially copying the CCPA had been introduced in other states, including Connecticut and Texas, but these were replaced by commissions or task forces to study the issue.

By mid-February 2021, bills had been introduced in five states (Minnesota, New York, Oklahoma, Virginia, and Washington). As noted above, the Virginia Consumer Data Protection Act was signed into law on March 2, 2021, and New York is also widely expected to pass legislation this year. This article reviews the new Virginia legislation, particularly by comparison to the CCPA. As legislative proposals in other states continue to progress, they will be reviewed in subsequent articles.

The Virginia Consumer Data Protection Act (HB 2307) tracks many of the consumer rights of the CCPA but differs in several important ways. One difference that has attracted vocal opposition from consumer groups is the lack of a private right of action in the Virginia law. Unlike the CCPA, the Virginia law also incorporates terminology borrowed from the GDPR of the EU, including personal data, controller and processor, with comparable definitions.

Exemptions

Exemptions under the Virginia law reflect key exemptions of the CCPA, but with important distinctions. First, and perhaps most significant, the CCPA exemptions for the personal information of personnel and business to

business contacts are limited in both scope and duration. Each of these exemptions is subject to a sunset provision currently scheduled for January 1, 2023. In addition, these exemptions do not apply to the CCPA requirements for reasonable security and its private right of action. In contrast, the Virginia law limits the definition of consumer to Virginia residents "acting only in an individual or household context" and excludes "a natural person acting in a commercial or employment context." As a result, the Virginia exemptions for personnel and business to business contacts are full and permanent.

The Virginia law also presents other important but subtle differences for the financial services and health care industries. The CCPA exempts (for the most part) (i) personal information collected pursuant to the Gramm-Leach-Bliley Act (GLBA); or (ii) protected health information collected by a covered entity or business associate subject to HIPAA, or to patient information collected by health care providers and treated in the same manner as protected health information subject to HIPAA. These CCPA exemptions do not apply to the obligation to provide reasonable security, or to the private right of action. In contrast, the Virginia law exempts in all respects financial institutions or data subject to the privacy provisions of the GLBA, and covered entities and business associates subject to HIPAA. These organizations and data are exempted completely, and the organizations covered by these exemptions do not need to consider for purposes of the Virginia law whether and to what extent they are processing information collected outside the GLBA and HIPAA regimes, as they do under the CCPA.

Consumer Rights

Similarly, consumer rights in the Virginia law correspond generally to those in the CCPA, but differ enough to present challenges to businesses that will be subject to both regimes. Differences include the Virginia law's right to correct personal data (which will be added to California law in 2023, when the CCPA amendments by the California Privacy Rights Act (CPRA) become effective); the private right of action that exists under the CCPA but not the Virginia law; and restrictions on processing personal data of minors, which apply in Virginia at 13 years old, and at 16 in California. Once the California amendments are effective, consumers will have rights against certain automated decision-making, a right not included in the Virginia law. Otherwise, consumers in both states will have the comparable right to know, right to access, right of portability, right to opt-out of sales, right to delete, and right of nondiscrimination.

Business Obligations

The obligations on businesses differ as well. Unlike the CCPA, the Virginia law restricts the purposes for which personal data may be collected to purposes "adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer." In addition, controllers cannot "process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal data is processed, as disclosed to the consumer," with consumer consent. The Virginia law also requires consumer consent for the processing of sensitive data. In contrast, effective in 2023 through the CPRA, the CCPA will provide consumer rights to restrict the use and disclosure of sensitive information, which is defined more broadly in California to include SSNs and other government identification numbers, and certain financial account information, as well as other types of information. Sensitive data is narrowly defined in Virginia to include information such as racial, ethnic, religious, mental and physical health, sexual orientation and citizen or immigration data; biometric and genetic information; personal data of a known child; and precise geolocation data.

Notices and Policies

The big question for most businesses that will be subject to both California and Virginia consumer privacy requirements: Can we use common forms of a privacy notice and privacy policy to comply with both statutes? Unfortunately, the answer is “it depends.” Because the Virginia notice and disclosure requirements are not as exacting as the California requirements under the CCPA and its implementing regulations, it is conceivable that the CCPA Notice at Collection and the CCPA Privacy Policy of a particular business could be adjusted to also cover the requirements of the Virginia Consumer Data Protection Act. Given the many gaps between the two statutes in definitions, exemptions and consumer rights, however, any business attempting to do so must use great care and careful analysis.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber