Published on *The National Law Review* https://natlawreview.com

Comprehensive State Privacy Laws On the Move, How Should Organizations Evaluate Them?

Article By:

Joseph J. Lazzarotti

Virginia may be the first state to follow California's lead on consumer privacy legislation, but it certainly will not be the last. The International Association of Privacy Professionals (IAPP) observed, "State-Level momentum for comprehensive privacy bills is at an all-time high." The IAPP maintains a map of state consumer privacy legislative activity, with in-depth analysis comparing key provisions. We discuss the Virginia legislation here, along with legislative activity in several other states that seem likely to pass. It was California that enacted the first data breach notification law which became effective in 2003. In about 15 years' time, all U.S. states have such a law, as well as many jurisdictions around the world.

Whether it is the pending Virginia Consumer Data Protection Act (VCDPA), the California Consumer Privacy Act (CCPA), or a similar framework, there are several features that should be considered when examining the effects of such laws on an organization:

- ***Does the law apply?*** Neither the CCPA nor the VCDPA apply to all organizations doing business in the state. But, they may apply more broadly than initially assumed, including organizations without locations in the particular state. Also, some entities that control or are controlled by covered businesses also could become subject to one of these laws even if such entities would not otherwise fall into the law's scope. Finally, data privacy and security laws increasingly reach third-party service providers to covered organizations either directly or indirectly through contracts that covered organizations must put in place.

- ***Are we exempt?*** Perhaps just as important as whether an organization is covered by one of these laws is the question of whether an exemption applies. It is important to know that while an organization may not be exempt as a whole, certain classifications data it maintains may be. For example, under the CCPA, "protected health information" covered by the Health Insurance Portability and Accountability Act (HIPAA) is generally exempt from the law. Of course, that information comes with its own compliance obligations!

- ***What is Personal Information?*** Assuming an organization is covered by the law, the next question it may want to ask is what data is covered. As we have discussed, there are various definitions and understandings of personal information. Similar to the CCPA and General Data Protection Regulation (GDPR), the VCDPA would define personal data broadly to

include “any information that is linked or reasonably linkable to an identified or identifiable natural person.” Again, this broad definition should be read together with potential exemptions to obtain a firm understanding of the information within the scope of the law’s protections. In some cases, such as under the GDPR, and the amendment to the CCPA, the California Privacy Rights Act, there is a subset of personal information that comes with even more protections. Often referred to as “sensitive personal information,” this category can include personally identifiable information such as racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, genetic or biometric data, and geolocation data. Of course, covered organizations with these categories of data would need to understand those additional requirements.

- ***Who is protected?*** It is not enough to know what kind of information that is “personal information,” covered organizations also need to know whose personal information is protected under the law. Several of these laws protect “consumers” defined generally as natural persons who reside in the jurisdiction. Basing the analysis solely on the word “consumer” and assuming that does not include employees, students, website visitors, etc. might be a mistake. Some frameworks have specific exclusions for these and other categories, others do not.

- ***What rights do protected persons have?*** Ostensibly, a key purpose for this kind of privacy legislation is to empower individuals with respect to their personal information. That is, to give them more access to and control over their data that is collected, used, disclosed, maintained, and sold . To effectively comply with these measures, covered organizations need to understand the kinds of rights granted. These rights can include:

    - The right to know what personal information is collected and processed, why, and to access such personal information

    - To right to correct inaccuracies in the personal information

    - To right to delete personal information

    - The right to limit processing of personal information

    - The right to opt out of the processing or sale of personal information

- ***Can my organization be sued for violations of the law?*** It is important to understand the consequences of failing to comply with any law. The flood of litigation under the Illinois Biometric Information Privacy Act (BIPA) which permits substantial recovery for failing to comply with notice and other requirements, even without a showing of actual harm, confirms the importance of examining this issue. Several of these privacy frameworks, including the CCPA and legislation supported by Governor DeSantis in Florida, include a private right of action in connection with data breaches.

- ***How will the law be enforced?*** Related to the question of whether consumers can sue for violations is how the law will be enforced, what are the potential penalties, and how are they measured. In most cases, enforcement rests with the state’s Attorney General’s office. Often, the law requires covered organizations be provided written notice of any violation and a period of time to cure the violation. Compliance can be challenging so covered organizations should be aware of a law’s enforcement scheme so that in cases where their compliance

efforts may not be perfect, they have a plan in place for quickly acting on such notices and curing any violations.

Answering these questions is certainly not the end of the analysis. For example, if covered, there are a whole host of additional questions organizations need to ask in order to evaluate compliance needs, allocate resources, identify affected business units, weigh risk management objectives, manage vendor compliance, and implement new policies and procedures, as needed. However, these questions can help to sharpen the big picture on the effect one or more of these privacy laws may have on your organization.

National Law Review, Volume XI, Number 49