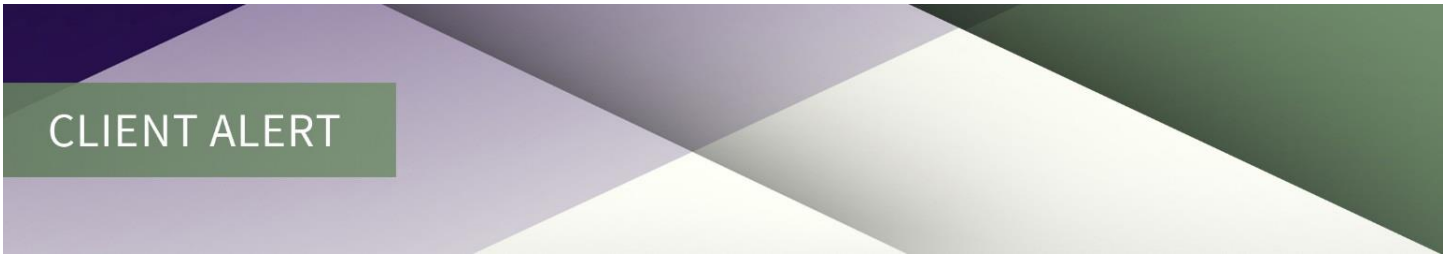

Six Months to Go: Preparing for the New and Updated Privacy Laws in California and Virginia

July 11, 2022

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Richard M Borden | Stefan Ducich

Introduction and Background

Over the last few years, privacy professionals have gained significant experience managing the uncertainties of a highly dynamic and constantly shifting regulatory and compliance landscape. Unfortunately, they will need to continue to lean on that experience, as the California Privacy Rights Act (the "CPRA") and the Virginia Consumer Data Protection Act (the "VCDPA") come into effect in just under six months, on January 1, 2023. While a number of unknowns persist, businesses need to start asking sometimes difficult questions—if they have not already started—about whether they are subject to these statewide comprehensive laws and what steps they will need to take to implement appropriate internal measures and public notices that meet any new obligations.

By way of background, the CPRA was adopted by California voters in November 2020 as an amendment to the California Consumer Privacy Act of 2018 (the "CCPA"). As we discussed here, CPRA expands consumers' rights to control their personal information, and requires businesses to implement and maintain new internal procedures and public-facing notices. On the heels of that effort, in March 2021, Virginia enacted the VCDPA, which protects consumer rights in a manner similar to the CPRA, although the scope of covered entities under VCDPA is slightly more limited. For more on the VCDPA, see here.

Roadmap to January 1: Preparing for CPRA and VCDPA

While the CPRA and VCDPA take similarly broad approaches to data protection, specific differences between the laws persist. As to the similarities, both require covered businesses to update public notices with specific practices (i.e., with respect to sensitive data), implement and maintain internal policies and procedures around specific processing, and to execute appropriate contractual agreements. And both are likely to (continue to) produce rules, regulations and/or guidelines for businesses to comply with the laws' provisions. However, the VCDPA and CPRA take different approaches to certain protections. For instance, each defines the scope of "sensitive data" differently (i.e., Virginia does not include government-issued ID, certain financial account information, union membership, sex-life information, or the contents of electronic communications where the business is not the intended recipient) and Virginia takes an opt-in approach to processing such data, whereas California takes an opt-out approach. State regulators have broadcast an intent to harmonize rules, but the lack of finalized rules complicates preparations.

There are certain questions that companies can ask to prepare for these state laws coming into force.

Are You Even Subject to the Laws?

Not every organization or company that collects data from California or Virginia persons will be subject to these laws. Both the CPRA and VCDPA set threshold requirements.

Like the CCPA before it, the CPRA applies to for-profit entities (i.e., "businesses") located or doing business in California, which collect personal information from residents of the state, and which meet the minimum processing or revenue thresholds. Under the CPRA, a regulated business is one that:

- Has an annual gross revenue of over $25 million;
- Buys, sells, or shares the personal information of at least 100,000 California consumers or households (up from 50,000 in the CCPA); or
- Derives more than fifty percent of its annual revenue from selling or sharing consumers' personal information.

The VCDPA applies to entities that conduct business in, or produce products or services targeted to residents of, Virginia, and which:

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

Understanding whether and how these laws apply to you will be a critical input to how you move forward.

What Data Do You Have and Where Does It Go?

Data inventories and data-mapping exercises were among the most helpful activities for companies preparing for the effective dates of the General Data Protection Regulation ("GDPR") in 2018 and the CCPA in 2020. Given aspects to these laws like the differential treatment of sensitive versus non-sensitive data in CPRA and the VCDPA, it will be important for companies that have never conducted such exercises to do so, and for those that conducted such exercises a few years ago, to update them.

Identifying the collection, use and disclosure of data, in particular with respect to "sensitive personal information," automatic decision-making, and targeted advertising, will be particularly important. All of these activities will likely feed into any analysis that you conduct related to whether to update consumer- and public-facing notices. And in Virginia, companies may need to conduct data protection assessments—understanding when those assessments need to happen and conducting them will be greatly facilitated by these other activities.

Are Your Vendor Contracts Compliant?

One of the key changes CPRA makes to CCPA is the addition of specific requirements around vendor contracts. While not as specific or potentially burdensome as GDPR's requirements for data processing contracts, these new requirements should help to ensure that a company is not unwittingly "selling" the data to the service provider.

Likewise, the VCDPA directs that any agreements with "data processors" (VCDPA imports terms like "data processor" from GDPR) to have agreements that "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." Like GDPR, the VCDPA includes specific terms that must be included in any such agreements.

Are You Ready To Respond to Consumer Requests?

One of the hallmarks of the GDPR that has been imported to the U.S. in state-level general privacy laws has been the codification of consumer (or "data subject") rights. While these concepts are not new to U.S. law—for example, some sector-specific laws include some of these rights—these state laws mark the first time that they have been generally available to the public for all personal information collected by covered companies.

The CPRA expands the consumer rights established under the CCPA; to meet these obligations, businesses will need to update both their public-facing notices and their internal procedures to respond to verified consumer requests.

Specifically, among other requirements, under the CPRA businesses must:

- Provide consumers the ability to correct inaccurate personal information;
- Provide "meaningful information about the logic" used in automated decision-making, as well as access and opt-out rights for such processing;
- Notify third parties with or to whom personal information has been shared, sold, or communicated upon receipt of verifiable requests to delete personal information;
- Provide consumers with notice and the ability to opt out if the business "shares"[1] personal information; and
- Disclose how "sensitive personal information"[2] is collected, used and disclosed, and provide consumers the ability to limit the use or disclosure of this information.

The VCDPA adopts similar rights—access, opt-out, deletion, correction, and portability. Companies will need to consider how to respond to any such requests, and whether to translate any differences between the CPRA and VCDPA into different approaches.

What About Employees?

One of the primary differences between CPRA and the other recently enacted state privacy laws, including VCDPA, is that the CPRA expands the laws' requirements to the employment context (including applicants for employment, contractors, etc.) whereas VCDPA and other state laws do not. Specifically, when the CPRA takes effect, the exemption under CCPA for the collection and processing of employee, applicant, and contractor personal information within the employment relationship is set to expire. This will extend consumer rights and protection obligations to such employee personal information. (Note, however, that certain proposed amendments currently under consideration by the California legislature arguably would, if enacted, either prolong the sunset provision to January 2026, or make the exemption permanent.) Companies need to consider how this change affects their operations and what additional steps they may need to take to comply.

[1] "Sharing" is the transfer or communication of consumer personal information to a third party for cross-context behavioral advertising.

[2] "Sensitive Personal Information" includes login credentials, precise geolocation information, biometric information, genetic and health data, social security number or other government-issued identification card number, and information related to race, ethnicity, religion, or sexual orientation.

What's Next?

Regulatory and enforcement authority under the CCPA was vested in the office of the California Attorney General ("CA AG"), which, since 2020, has issued certain rules pursuant to, and guidelines regarding, the law; however, this authority has now been transferred to the newly established California Privacy Protection Agency ("CPPA") (although the CA AG may still bring enforcement actions under CPRA). The CPPA is in the early stages of exercising its rulemaking authority—on July 8, 2022, the CPPA issued a Notice of Proposed Rulemaking[3] along with the proposed regulations,[4] triggering a 45-day public comment period—and we expect the agency to issue regulations in several areas as we approach January 2023 and beyond. Even as companies take steps to comply with CPRA as they understand it today, they will need to monitor proceedings at the CPPA and guidance from regulators in Virginia to make sure those are appropriately incorporated into their compliance efforts.

Companies should also keep these questions in mind as new comprehensive privacy laws are set to come into effect in Colorado, Connecticut, and Utah beginning July 1, 2023.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Richard M. Borden
12 728 3872
rborden@willkie.com

Stefan Ducich
202 303 1168
sducich@willkie.com

[3] The Notice of Proposed Rulemaking is available here.

[4] The Proposed Regulations are available here.