Articles + Publications | March 4, 2021

Introduction and Overview: Virginia Consumer Data Protection Act Series (Part One)

WRITTEN BY

Ronald Raether, Jr. | David N. Anthony | Ashley L. Taylor, Jr. | Sadia Mirza | Julie Hoffmeister Smith | Edgar Vargas

Download PDF

We have long predicted that just as other states followed California in passing breach notification laws, states would follow in California's footsteps in regulating information privacy practices with the California Consumer Privacy Act of 2018 (CCPA), which was later amended by the California Privacy Rights Act of 2020 (CPRA).[1] The Virginia state legislature recently became the first state to do so, surprising many with news that it quickly passed and signed into law comprehensive privacy legislation, namely the Virginia Consumer Data Protection Act (CDPA). Like the CCPA, Virginia's CDPA builds on the Fair Information Practice Principles (FIPPs), making many of the lessons learned implementing the CCPA applicable here. The CDPA will take effect January 1, 2023.

This five-part series on Virginia's CDPA provides a detailed overview of the act, and how it compares to California's approach to privacy under the CCPA and CPRA. The series will be divided into the following parts:

1. Introduction and Overview
2. Consumer Rights
3. Notice and Disclosure Obligations
4. Data Processing Obligations
5. Enforcement

At the conclusion of the series, Troutman Pepper will host a webinar on the Virginia CDPA. Registration information will be circulated at a later date.

A. Why Virginia's CDPA is Similar to California's CCPA

It should come as no surprise that Virginia's CDPA is similar, but not identical to, California's CCPA. Indeed, as we discussed in our 2019 *Bloomberg Law* article, *So the CCPA is Ambiguous – Now What?*, all privacy laws derive from the same core foundational principals, namely the Fair Information Practice Principles (FIPPs). This includes, for example, the CCPA, CPRA, Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), Health Insurance and Portability and Accountability Act of 1996 (HIPAA), Driver's Privacy Protection Act (DPPA), and even Europe's General Data Protection Regulation (GDPR).

Intended as guidelines that represent how organizations should collect and use personal information, the FIPPs recommend certain safeguards to ensure data collection practices are fair, and businesses are being transparent about their privacy practices. To this end, the FIPPs focus on adopting privacy frameworks that incorporate principles of *notice*, *choice*, *access*, and *security*. Because all privacy laws derive from these same core principles, it makes sense why we often see similar obligations and terminology across the different privacy laws. Notably, Virginia's CDPA borrows much of its terminology from Europe's GDPR (*e.g.*, the terms "controller" and "processor"), but also incorporates much of the text of the CCPA.

From a practical perspective, businesses seeking to comply with Virginia's CDPA should consider how these other privacy laws have been interpreted and enforced in the past.[2] By doing so, many of the challenges organizations may face with Virginia's CDPA — especially in the absence of implementing regulations — may become less obscure and enable organizations to make informed, well-reasoned compliance decisions still in line with their business goals.

B. Scope of Application: Who's Covered?

If your organization falls under the CCPA, then you know the CCPA primarily regulates "businesses." If you started your CCPA-compliance journey with Troutman Pepper, you may recall our infographic that breaks down the definition of a CCPA-regulated business, available here. In short, a CCPA-regulated "business" is any organization that (a) operates for the profit or financial benefit of its shareholders or other owners, (b) collects California consumers' personal information, (c) either alone or jointly with others, determines the purposes and means of the processing of consumers' personal information, and (d) meets certain threshold requirements.[3]

Entities that process personal information on behalf of regulated business are referred to as "service providers." While the obligations imposed on businesses by the CCPA are direct, a service provider's obligations under the CCPA are generally defined by the business in the applicable service provider contract.

For all practical purposes, a "business" under California's CCPA equates to a "controller" under Virginia's CDPA. Similarly, a "service provider" under California's CCPA corresponds to a "processor" under Virginia's CDPA. Those who deal with the GDPR will be familiar with these terms.

Entities are subject to the Virginia CDPA if they conduct business in the commonwealth or produce products or services that target residents of the commonwealth, and that:

- during a calendar year, *control* or *process* personal data of at least 100,000 consumers[4]; or

- *control* or *process* personal data of at least 25,000 consumers and derive over 50% percent of gross revenue from the sale of personal data.

Notably, Virginia's CDPA provides a "blanket exemption" from the act for (1) government agencies and authorities, (2) financial institutions subject to the GLBA, (3) "covered entities" or "business associates" regulated by HIPAA and HITECH, (4) nonprofit organizations, and (5) institutions of higher education. This differs slightly from California's approach, which provides an "information exemption" in certain contexts — meaning data regulated by certain laws, such as the GLBA and FCRA are exempt — but the entity itself may still be covered.

The below chart provides a comparison of the "blanket exemptions" under California's CCPA and CPRA and Virginia's CDPA.

C. Scope of Application: What Information is Regulated?

"Personal information" under California's CCPA equates to "personal data" under Virginia's CDPA. Both terms essentially mean any information linked or reasonably linkable to an identifiable person. Both California and Virginia exclude from the scope of their laws (1) information regulated by certain other privacy laws and (2) information that meets each state's definition of "de-identified" and "publicly available" information. Below find a high-level overview of the types of information that falls outside the scope of "personal information" under California's CCPA and CPRA and "personal data" under Virginia's CDPA.

Although not present in California's CCPA, both the California CPRA and Virginia CDPA introduce the concept of "sensitive" information/data and impose certain requirements relating to such. This follows Europe's GDPR approach, which provides specific protections when "special categories of personal data" are involved.

D. Consumer Rights

The second part of this series will cover the new consumer rights created by Virginia's CDPA, and how such rights differ in comparison to those offered under California's CCPA and CPRA. The below chart previews how the two states differ with respect to this issue.

E. Notice and Disclosure Obligations

The third part of this series will cover the notice and disclosure obligations imposed by Virginia's CDPA, and how such obligations compare to those imposed by California's CCPA and CPRA. The below chart previews how the two states differ with respect to these issues.

F. Data Processing Obligations

Service providers, and processors, and contractors, oh my! The fourth part of our series will detail the processing obligations imposed by Virginia's CDPA, and how such obligations compare to those under California's CCPA and CPRA. The article will focus on issues relating to data assessments and requirements relating to data minimization, obtaining affirmative consent to process certain types of information, and vendor contracts.[5] The below chart provides a high-level overview how the two states differ with respect to these issues.

G. Enforcement

We will put organizations out of their misery now and reveal that, like California's CCPA and CPRA, there is no private right of action for a violation of Virginia's CDPA. This was a contentious issue under the CCPA despite the statute's plain and unambiguous language, which provides that the California attorney general holds sole enforcement authority for CCPA violations but confers a private right of action in the data breach context.[6]

Part five our series will take a deep dive into the enforcement provisions of Virginia's CDPA, and how such provisions compare to those under California's CCPA and CPRA. For now, see our preview chart below on how Virginia's approach compares to California's.

[1] Unless stated otherwise, the term "CCPA" is intended to reference the CCPA and CPRA in general. Where we felt it was necessary to draw a distinction between the CCPA and CPRA, we did so by explicitly stating such.

[2] *See*, for example, Troutman Pepper's CCPA Enforcement Series, which identifies six areas of enforcement likely to catch the California office of the attorney general's attention.

[3] In order to qualify as a "business" under the CCPA, the business must also meet one or more of three thresholds: (1) the business has annual gross revenues in excess of $25 million dollars; (2) the business alone, or in combination, annually buys, receives for the businesses' commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more California consumers, households, or devices; or (3) derives 50% or more of its annual revenues from selling consumers' personal information. *See* Cal. Civ. Code § 1798.140(c). The CPRA slightly modifies threshold (2) by increasing the threshold from 50,000 to 100,000.

[4] "Consumer" means a natural person who is a resident of the commonwealth acting only in an individual or household context. It does not include a natural personal acting in a commercial or employment context.

[5] For organizations interested in learning more about the CCPA's obligations with respect to vendor contracts, see our *Law360* article titled, "Calif. Privacy Law Means New Approach to Vendor Contracts."

[6] A race to enforcement appears to be on the horizon. In Illinois, H.B. 3910 would grant the state attorney general enforcement powers, while H.B. 2404 would provide individuals with a private right of action. Massachusetts' S.B. 1726 would establish a state information privacy commission to handle enforcement. Minnesota's H.B. 1492 and Utah's S.B. 200 would empower the attorney general the power to take enforcement action against violators.

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services
- Privacy + Cyber
- State Attorneys General