Articles + Publications | March 18, 2021

Notice and Disclosure Obligations: Virginia Consumer Data Protection Act Series (Part Three)

WRITTEN BY

Ronald Raether, Jr. | David N. Anthony | Ashley L. Taylor, Jr. | Jon S. Hubbard | Timothy J. St. George | Noah J. DiPasquale | Sadia Mirza

Download PDF

One key area where Virginia's Consumer Data Protection Act (CDPA) differs from the California Consumer Privacy Act of 2018 (CCPA) and the California Privacy Rights Act of 2020 (CPRA)[1] is the law's notice and disclosure obligations.

In this third installment of our five-part series on Virginia's CDPA, we will review the contours of the law's notice and disclosure requirements, compare and contrast them with the requirements of California's CCPA and CPRA, and give helpful guidance to businesses seeking to ensure compliance with Virginia's new law.

As we explained in our prior installments, each of these privacy laws is based on the Fair Information Practice Principles (FIPPs), which include the principle that a consumer should be given notice of information practices before personal information is collected. However, each law differs in the kind, form, and extent of the notice that it obligates regulated entities to provide. The chart below previews how the Virginia and California laws differ with respect to these issues:

These commonalities and distinctions are detailed further below.

A. The Notice/Disclosure Differences Between Virginia's CDPA and California's CCPA

The California CCPA imposes several notice and disclosure obligations on regulated businesses, derived from multiple interrelated, cross-referenced provisions of the law. These include:

1. **Privacy Policy.** A comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information, and the rights of consumers regarding their personal information.

2. **Notice at Collection.** A notice to provide consumer with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, and the purposes for which the personal information will be used.

3. **Notice of Right to Opt Out.** A notice to inform consumers of their right to direct a business that "sells" their personal information to stop selling their personal information.

4. **Notice of Financial Incentive.** A notice of the material terms of any financial incentives the business offers to consumers as compensation for the collection or sale of personal information (*e.g.*, coupons or special promotions that require sharing personal information for participation) so that the consumer may make an informed decision about whether to participate.

By contrast, the notice and disclosure requirements of Virginia's CDPA are *much* more streamlined and contained in a single section of the law titled, "Data controller responsibilities; transparency," § 59.1-574(C)-(E). In short, the Virginia CDPA requires only that a regulated "controller" provide a privacy notice to consumers, which includes certain listed information and, if applicable, a "clear and conspicuous" disclosure of the sale of personal information to third parties or use of personal information for targeted advertising and how the consumer may opt out of both.[2] This privacy notice requirement is most similar to the CCPA's "privacy policy" requirements. Notably, Virginia's CDPA *does not* require a separate notice at collection; does not require a separate notice of the right to opt out; and does not require notice of financial incentives.

The below breaks down the timing, form, and content of the privacy notice required by Virginia's CDPA.

B. Timing of Virginia CDPA Privacy Notice

Unlike the CCPA's "Notice at Collection" requirements, which require businesses to provide notice "at or before the point of collection," Virginia does not specify when the CDPA privacy notice must be provided to consumers. Rather, Virginia's CDPA simply requires controllers to provide consumers with a "reasonably accessible, clear, and meaningful" privacy notice, without specifying any timing requirements. That leaves the details of compliance somewhat open to interpretation, but suggests that Virginia's CDPA does not obligate controllers to provide a "just-in-time" notice. That is, there is no explicit requirement that Virginia's CDPA privacy notice be provided "at or before the point of collection."

C. Form of Virginia CDPA Privacy Notice

As noted above, Virginia's CDPA requires controllers to provide a privacy notice to consumers that is "reasonably accessible, clear, and meaningful." By comparison, the California CCPA requires a privacy policy "in a form that is reasonably accessible to consumers," and expressly specifies that for privacy policies provided online, the business will follow generally recognized industry standards, such as the World Wide Web Consortium's "Web Content Accessibility Guidelines," Version 2.1 of June 5, 2018. CCPA also requires the privacy policy to be posted online through a conspicuous link using the word "privacy" on the business's internet homepage or landing page of a mobile application, and instructs businesses that do not operate a website to make the privacy policy "conspicuously available to consumers."

The Virginia CDPA does not expand on what qualifies as "reasonably accessible, clear, and meaningful." Even in the absence of clarifying language, however, organizations should consider taking the following steps:

1. **Avoid Legal Jargon.** Use plain, straightforward language, avoiding technical or legal jargon.

2. **Adopt a Layered Format.** Use a format that makes the notice readable, such as a layered format.

3. **Post It Prominently and Use a Descriptive Title.** Make the notice recognizable by giving it a descriptive title. In the case of a website, consider using a conspicuous link on your homepage containing the word "privacy." Make the link conspicuous by using larger type than the surrounding text and contrasting color symbols to call attention to it. Additionally, consider putting a conspicuous "privacy" link on every webpage where personal information is collected. In the case of an online service, such as a mobile application, consider posting or linking to the notice on the application's platform page, so that users can review the notice before downloading the application.

4. **Option to Print.** Format the notice so that it can be printed as a separate document.

5. **Consider Readability.** Use a format that makes the notice readable, including on smaller screens, such as on a mobile device.

6. **Consider Alternative Means.** For organizations that do not have a web presence, consider methods to inform consumers about how they can learn about your data collection and sharing practices.[3]

D. Content of Virginia CDPA Privacy Notice

Virginia's CDPA requires that a privacy notice include the following information:

1. The categories of personal data processed (CCPA refers to categories of data "collected" — there is likely no practical difference for the purpose of the privacy notice/privacy policy);

2. The purpose for which personal data is processed;

3. The way a consumer may exercise his or her rights under the CDPA, including how to appeal the controller's

decision regarding a request to exercise them;

4. The categories of third parties the controller shares personal data with, and the categories of personal data shared with those third parties;

5. A description of one or more secure and reliable means for consumers to submit a request to exercise their consumer rights under the CDPA;[4] and

6. If the controller sells personal data to third parties or uses personal data for targeted advertising, a "clear and conspicuous" disclosure of that sale or use and the means to opt out. It is notable that the Virginia legislature chose to use the phrase "clearly and conspicuously" regarding the third-party sale and targeted advertising disclosure. The use of this language may suggest that this disclosure, where applicable, should be presented in a form distinguishable from the rest of the notice. This may be accomplished by using a bold or darker font, larger type, or a separate labelled section within the larger privacy notice.

Unlike California CCPA privacy policy requirements, the Virginia CDPA privacy notice does not need to include, among other things: (1) the sources from which personal data is collected; (2) a description of the process that will be used to verify consumer requests; (3) metrics on the number of consumer requests received, complied with, and denied in the previous calendar year; and (4) a description of a consumer's rights under the CDPA. With respect to the last point, however, the Virginia CDPA does require the privacy notice to describe "one or more secure and reliable means" for a consumer to request to exercise his or her rights, which may by implication warrant a disclosure of the rights available to a consumer under this law.

The following chart provides a high-level overview of the content requirements required by each law.

E. The Infamous CCPA "Do Not Sell" Button

Another major difference between California's CCPA and Virginia's CDPA are the required notices regarding the sale or sharing of personal data with third parties, and the consumer's right to opt out of them. The California CCPA requires a business to include on its internet homepage a "clear and conspicuous link" enabling the consumer to opt out of the sale of the consumer's personal information to third parties (commonly referred to as a "Do Not Sell" button). The California CPRA expanded the scope of this requirement to include sharing of personal information with third parties for cross-context behavioral advertising (*i.e.*, a "Do Not Sell or Share" link).

On this subject, the Virginia CDPA does not require controllers to implement a "Do Not Sell" link on their internet homepages. Instead, a controller engaging in either (1) the sale of personal data to third parties; or (2) the use of personal data for targeted advertising must disclose these practices and how a consumer may opt out. The provision requiring this disclosure provides no instructions as to the timing or format of this disclosure. Given its statutory location in between provisions relating to the privacy notice, however, and the lack of any other instruction as to where to post or when to provide it, this disclosure likely is intended to be included in the privacy notice.

F. A Path Forward

The California CCPA and Virginia's CDPA differ in many ways. Consumer notice and disclosure obligations are one area at least where Virginia's CDPA is notably more streamlined and straightforward.

On the other side of that same coin, however, the Virginia's CDPA provisions offer much less detail than the CCPA, leaving some important questions unanswered. Because the CDPA is based on the same core principles as other privacy laws (*i.e.*, the FIPPs), businesses would be doing themselves a disfavor if they did not consider how the notice and disclosure obligations included in other privacy laws — including California's CCPA — have been interpreted and enforced in the past. By doing so, many of the challenges organizations may face in implementing the Virginia' CDPA privacy notice requirements may become less obscure, and organizations will be able to make compliance decisions that are informed, well-reasoned, and still in line with their business goals.

---

[1] The CPRA amended the CCPA in 2020. Except where specifically noted, both are referred to collectively as the CCPA hereafter.

[2] For information comparing a CCPA-regulated "business" to a CDPA-regulated "controller," see Part One of this series, which provides an introduction to and overview of the Virginia CDPA.

[3] The guidance provided in this section is borrowed from the California attorney general's guidance on "Making Your Privacy Practices Public," which can be accessed here.

[4] Similar to the CCPA, Virginia's CDPA provides guidance as to what constitutes a "secure and reliable means," instructing businesses to consider (1) the ways a consumer normally interacts with the business, (2) the need for secure and reliable communication of the request, and (3) the ability to authenticate the identity of the consumer

making a request.

RELATED INDUSTRIES + PRACTICES

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