9

Vanguard States: California, Colorado, Nevada, Virginia, and . . .?

A handful of U.S. states have enacted their own state-specific privacy laws that, while a patchwork, for now create de facto national standards. The California Consumer Privacy Act (CCPA) took effect on January 1, 2020. California continues to lead in this area, with its voters approving a ballot initiative known as Proposition 24, or the California Privacy Rights Act (CPRA), in 2020. The CPRA consists of a package of amendments to the CCPA that will take effect on January 1, 2023. On the same date, comprehensive privacy laws recently enacted by Virginia and Colorado also will take effect. Nevada has also recently expanded its privacy statute. In recent years, multiple other states—including Florida, New York, and Washington—have seriously considered comprehensive privacy bills. It seems likely that at least some of these states will pass such bills within the next few years.

This chapter briefly summarizes what the legislatures of California, Colorado, Nevada, and Virginia have passed as well as legislation that other states have considered but have not yet passed. Readers are encouraged to watch the news for updates on all topics covered by this book, as privacy law is highly dynamic, and state legislatures are active in this arena.

The California Consumer Privacy Act (CCPA)

Applicability & Definitions

Q 9.1 To which organizations does the CCPA apply?

The CCPA applies to for-profit businesses doing business in California that meet one of the following three criteria: (1) have $25 million in annual revenue; (2) transact with more than 50,000 California residents' data annually; or (3) derive 50% or more of annual revenue from selling the data of California residents.[1] The revenue threshold is global, not California-specific, and will be increased every two years based on the U.S. Consumer Price Index. Note that $25 million in global revenue is all it takes for a for-profit organization to be covered—even if it does not meet the numerical threshold of California residents transacted with annually. On January 1, 2023, the second factor for applicability—transacting with more than 50,000 California residents—will increase to 100,000 residents, signaling that the CCPA is intended to impose obligations on larger organizations and aligning the CCPA with new privacy laws adopted in Colorado and Virginia.

Q 9.1.1 Are any regulated industries exempt from the CCPA?

There is no blanket exemption for financial institutions subject to the Gramm-Leach-Bliley Act (GLBA). (See chapter 4 for more on financial institutions generally.) Healthcare entities subject to the Health Insurance Portability and Accountability Act (HIPAA) do enjoy a very broad exemption from CCPA as a practical matter, given certain carveouts from CCPA.[2] (See below and chapter 5 for details.)

Q 9.1.2 Does the CCPA apply to service providers who might have consumer data?

Yes. The CCPA defines a service provider as an entity "that processes information no behalf of a business and to which the business discloses a consumer's personal information for a business purposes pursuant to a business contract."[3] The contract between the business and the service provider must prohibit the service provider from retaining, using, or disclosing personal information other than for the business purposes specified in the contract.

In addition to the statutory text, companies seeking to comply with the CCPA also must consider the implementing regulations issued by the California Attorney General.[4] The CCPA regulations provide that service providers "shall not retain, use, or disclose personal information obtained in the course of providing services except" in certain circumstances. These circumstances include:

(1) Processing or maintaining "personal information on behalf of the business that provided the personal information or directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA";

(2) Retaining a subcontractor, "where the subcontractor meets the requirements for a service provider under the CCPA and these regulations";

(3) Internal use by the service provider;

(4) Detecting "data security incidents or protect against fraudulent or illegal activity"; or

(5) Circumstances otherwise permitted by certain sections of the CCPA.[5]

Notably, a service provider is prohibited from selling data on behalf of a business after the consumer has opted out of the sale of personal information and may respond on behalf of the covered business or re-direct the consumer to the covered business.[6]

Q 9.2 What kind of data is covered by the CCPA?

The CCPA applies to "personal information," which is defined very broadly. Any data that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" is covered.[7] One can think of it as a "breadcrumbs" definition—whatever data might reasonably form a trail leading back to the consumer appears to be covered. The Act's definition specifically references, for example, Internet activity, geolocation data, employment-related information, consumer purchase histories, biometric data, and even "olfactory" information. Going even further, the Act also defines as "personal information" any "inferences" that could be drawn from any of the listed categories of personal information to create a profile.[8]

In September 2019, the California legislature passed and the governor signed certain amendments to the CCPA. One of the amendments clarifies that "personal information" under the CCPA is subject to a reasonableness requirement. In order for information that does not directly identify a consumer to be within scope, that information must "reasonably" be capable of being associated with a consumer or household. The mere possibility that the information can be linked to an individual is not enough.

Q 9.2.1 Are any types of data exempt from the CCPA?

The CCPA was amended in September 2018 to provide exemptions for specified types of information. The amendments exempt the following types of information:

- "[P]rotected health information" collected by "a covered entity or business associate" governed by HIPAA's privacy, security, and breach notification rules as well as "medical information governed by [California's] Confidentiality of Medical Information Act."
- "Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the 'Common Rule.'"
- "[P]ersonal information collected, processed, sold or disclosed pursuant to" the GLBA and its implementing regulations and information governed by the California Financial Information Privacy Act (FIPA).
- "[P]ersonal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994."[9] A company may be covered by the information-based exemptions for some purposes and not others—that is, it may collect and use certain information in a way that is exempt from, and other information in a way that is still subject to, the CCPA. For example, not all information handled by a financial institution is necessarily handled "pursuant" to GLBA.

Additionally, one of the September 2019 amendments exempts employment information from the CCPA's scope that is collected about a California resident in their role as "a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor" of the covered business. Emergency contact information for employees also is exempted under the amendment, as well as personal information necessary for the covered business "to administer benefits" for the employee's dependents or beneficiaries.

There are two caveats to this exception: (1) covered businesses must still disclose to employees (and to applicants, etc.) at or before the point of collection the categories of personal information they collect; and (2) this exemption does not apply to the CCPA's private right of action for data breaches. Employees, like consumers, will be able to sue, and recover generous statutory damages, if their personal information is compromised.

Also exempted under the September 2019 amendments is personal information "reflecting a written or verbal communication or a transaction between" a covered business and a consumer who is acting "as an employee, owner, director, officer, or contractor" of another company, where the covered business is engaged in "conducting due diligence regarding, or providing or receiving a product or service" from the other company. This exemption does not apply to one of the provisions concerning the consumer's right to opt out of the sale of their data, the anti-discrimination provisions, or the private right of action for data breaches.

The September 2019 amendments also create an exemption for certain activities regulated by the Fair Credit Reporting Act and an exemption—from the do-not-sell right—for vehicle information and vehicle ownership information shared between a motor vehicle dealer and the vehicle's manufacturer. These exemptions do not apply to the private right of action for data breaches.

Originally, the CCPA included "sunset" provisions on the exemptions for personal information associated with employees and in the context of business-to-business transactions that would have made these exemptions ineffective on January 1, 2021. The CPRA extended these provisions until January 1, 2023.

Q 9.2.2 How broad is the GLBA exemption under the CCPA?

The federal GLBA exemption and FIPA exemption apply to information, not institutions. Financial institutions thus will be well advised to consider, dataset by dataset, whether their data is covered by GLBA or FIPA. One critical component to understanding the reach of the exemption is examining the definitions of "consumer" and "personal information" under the CCPA, on the one hand, and "consumer" and "nonpublic personal information" under GLBA, on the other.

A consumer is an individual who obtains a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes. The GLBA Privacy Rule protects a consumer's "nonpublic personal information." Nonpublic personal information is "personally identifiable financial information" that:

- is "provided by a consumer to a financial institution";
- "[r]esult[s] from any transaction with the consumer or any service performed for the consumer"; or
- is "otherwise obtained by the financial institution."[10]

The Privacy Rule defines "personally identifiable financial information" as information:

- that a consumer provides to a financial institution "to obtain a financial product or service" from the financial institution;
- "about a consumer resulting from any transaction involving a financial product or service" between the financial institution and a consumer; or
- that the financial institution "otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer."[11]

Q 9.2.3 What information would likely fall under the GLBA exemption?

The core data generated in opening a financial account, or servicing it day to day, will likely be exempt. For example:

- Receiving and reviewing a loan application for a family car from a consumer.
- Opening a credit card with a financial institution for personal, family, or household purposes.
- Opening a checking or savings account for personal, family, or household purposes.[12]