The California Consumer Privacy Act

July 31st, 2019 | and Patricia E.M. Covington

Patricia E.M. Covington, Meghan Musselman and Nora Udell

The California Consumer Privacy Act of 2018 ("CCPA") was signed into law on June 28, 2018 and will take effect on January 1, 2020. The enforcement date – the first date on which the Attorney General may bring an enforcement action under the CCPA – is July 1, 2020 or six months after the publication of the Attorney General's final regulations, whichever is sooner. As of today, the Attorney General's regulations have not been released and several amendments to the CCPA are pending before the California legislature, leaving much uncertainty surrounding compliance with the law.

The CCPA is best understood as a consumers' bill of rights that sets out a consumer's right to: (1) know what information a business collects and sells, (2) access the information collected, (3) demand deletion of the information that is collected, (4) opt out of the sale of the information, and (5) be free of discrimination based on the assertion of CCPA rights. As such, compliance with the law does not merely require consumer disclosures. Rather, compliance will affect how businesses collect, retain, share, and manage consumer data.

This article will summarize the scope of the CCPA and its data-specific Gramm Leach Bliley Act ("GLBA") exemption, note several questions left unanswered by the statute, and explain why data mapping and data hygiene are critical steps your business can take now to ready itself for CCPA compliance in 2020.

Scope of the CCPA and the GLBA exemption.

The CCPA applies to businesses that collect or sell consumers' personal information. "Business," "collect," "consumer," and "personal information" are defined broadly by the CCPA and are far-reaching. And for every definition, the CCPA leaves open important questions.

A "consumer" is a natural person who is a California resident, however identified, including by any unique identifier. A "resident" includes every individual who is in California for other than a temporary or transitory purpose, and every individual who is domiciled in California who is outside of California for a temporary or transitory purpose.[1] The expansive definition of consumer means that businesses cannot merely designate persons physically located in California as covered by the CCPA, because the term includes California residents who are physically outside of California too.

A "business" is a legal entity doing business in California, that collects consumers' personal information or on whose behalf the information is collected, that satisfies one or more of the

following thresholds:

- Has annual gross revenues in excess of twenty-five million dollars.
- Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
- Derives 50% or more of its annual revenues from selling consumers' personal information.[2]

Adding to the expansiveness of the definition of "business," it is not clear that "households" and "devices" are limited only to California residents' households or devices.[3] As such, the second criteria of "50,000 or more consumers, households, or devices" may apply to businesses that handle the personal information of 50,000 or more households or devices, nationally.

"Collecting" personal information means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior. The definition does not include retention requirements, meaning that even if a business does not retain information that it actively or passively accesses, it may still be subject to the CCPA.

"Selling" personal information means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.[4] Valuable consideration is not defined by the CCPA but appears to include more than merely the exchange of consumer personal information for money.

"Personal Information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.[5] The CCPA provides a nonexclusive list of examples of personal information, including IP addresses, "purchasing or consuming histories or tendencies," and "[i]nferences drawn from any of the information identified [ ] to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[6] The examples of "personal information" make clear that the CCPA gets at information that is not only provided by consumers to businesses, but that is inferred about consumers by businesses. However, the information is "personal information" under CCPA only if it "identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."[7]

The CCPA does ***not*** exempt financial institutions that are subject to the federal Gramm-Leach-Bliley Act ("GLBA"). Rather, the CCPA exempts personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act ("GLBA").[8] Remember that the GLBA exemption will not exempt personal information collected by a business in the context of a commercial purpose transaction because the GLBA does not govern commercial purpose financial products or services.

Because the GLBA exemption is data-specific, not entity-specific, any business could hold data subject to the GLBA exemption **and** data not subject to the GLBA exemption. This means that any business may hold data that is subject to the CCPA and that is exempt from the CCPA.

Data Mapping and Data Hygiene

The only way to know if your business's consumer data is subject to the CCPA or exempt from the CCPA under the GLBA exemption, is to know what data your business collects, uses, stores, shares and sells. Remember that collecting includes data your business has access to, even if it does not retain it. This requires data mapping, or a similar process of inventorying and understanding the flow of data into, within, throughout, and out of your organization-from cradle to grave.

The inventorying component of data mapping involves uncovering or finding the data and then classifying it. In this effort, a business identifies where the data "lives"-*all the places* where it can be found and/or accessed. This include all mediums (*e.g.*, electronic and physical) and channels (*e.g.*, online, telephone, in-person). For example, considering all IT systems, servers, devices, filing cabinets, physical locations and storage places where the data is maintained.

The next step requires identifying and understanding the flow of the data-where does it go, what is done with it, how is it used, who has access to it, etc. For example, is the data shared with third-parties, and if so, with whom, and what do they do with the data? Does the third-party share the data with another third-party? Think of it as a who, what, when, where, why and how exercise. Through this process, your business can tag data as being within the GLB exemption or outside of it. Once tagged, your business will be in a position to determine what its obligations are with respect to its data under the CCPA. An organization would be wise to take advantage of this effort and identify who has access to the data and why. The CCPA is likely the first of many different types of data privacy and security measures. Data privacy and security are becoming more like "fundamental rights," and these rights are likely to increase.

Data mapping is a multi-disciplinary, collaborative effort-no one person or department can complete it on her own. Representatives across the business must be involved, from legal and IT to HR, the different business lines, marketing, risk management and other departments that use and/or "touch" consumer data. Data mapping is an ongoing process. Practices and procedures will change, requiring businesses to update their mapping. For example, when your business begins sharing information with a new service provider, that information must be incorporated into the map. Data mapping is critical-only when you know what data you have, how you got it, why you have it, where it lives, how you use it, and how and with who you share it-can you decide if the data is subject to the CCPA.

As part of this process, a business should also consider its data hygiene. In this context, data hygiene involves critically assessing whether the data that is collected, used, stored, shared, etc. is even necessary. And, if necessary, whether such collecting, using, storing, sharing, etc. is limited to those circumstances and places required to achieve the intended purposes and/or objectives. Put simply, is your business collecting or retaining information unnecessarily? Careful consideration of what consumer information your business needs, purging what it doesn't, and an overall "slimming down" of where the data lives will go a long way in reducing the complexity of CCPA compliance and data security risk.

---

[1] Section 1798.140(g); 18 CCR § 17014.
[2] Section 1798.140(c).
[3] *See* Section 1798.140(j).

[4] Section 1798.140(e).
[5] Section 1798.140(o).
[6] *Id.*
[7] *Id.*
[8] Section 1798.145(e).