The California Consumer Privacy Act of 2018 ("CCPA") and How It Affects Your Service Provider Agreements

A Beginner's Guide

Kevin DiLallo & Patrick Whittle
April 30, 2019

It's long been known that U.S. regulation of enterprises' handling of personal information (PI) they collect is – except for specialized circumstances – light-handed. To be sure, some specialized requirements exist. Health information is subject to specific regulation under the Health Information Portability and Accountability Act (HIPAA); financial institutions have particular obligations under the Gramm-Leach-Bliley Act, and children's online privacy is protected by the Children's Online Privacy Protection Act (COPPA). In all other cases, though, there has been little or no federal legislation dictating corporate procedures for handling PI. Responsible enterprises that do business online (and who doesn't?) have privacy policies that describe their methods and procedures for handling PI, which they make accessible to consumers both online and through other means. But until now, generally, companies have been free to set the specific terms of their privacy policies. The Federal Trade Commission ("FTC") brings enforcement actions when companies violate their own policies but otherwise provides only non-binding, high-level "principles" for what such policies should ideally contain: know what PI you have; don't keep more than you need; protect what you keep; dispose properly of what you no longer need; and create a plan for dealing with security breaches. The FTC has characterized its guidance to enterprises as "Say what you do, and do what you say."

Companies doing business in Europe know that EU regulation is significantly stricter, and there have been pushes from time to time for the U.S. to adopt similarly strict measures. Now the largest state, California, has passed legislation along European lines. The California Consumer Privacy Act of 2018 (CCPA) is set to take effect January 1, 2020, though it may take up to six months more for the state Attorney General to adopt implementing regulations. The latter period only affects the state's ability to bring enforcement actions; private parties can sue for violations as of January 1, 2020.

Brief Overview of the CCPA

For all intents and purposes, the CCPA applies to all for-profit enterprises ("businesses") of any size who do business in California. A business is exempt *only if* it meets all the following criteria: (i) it has annual gross revenues less than $25,000,000; (ii) it buys, receives, shares or sells PI for fewer than 50,000 consumers, households, or devices; (iii) it derives less than 50% of its revenues from selling personal information;

and (iv) it doesn't co-brand with, or fall under the same corporate control as, another entity that fails to meet one or more of the above requirements.

"Personal Information" Under the CCPA

To understand these requirements, it is first necessary to note that the CCPA defines PI very broadly. The term includes any 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." Thus, even information that does not name the consumer directly but can merely be associated with, or linked to, the consumer, is covered. The CCPA lists (but doesn't limit itself to) several examples of such information. Besides the obvious examples, PI also includes:

- Internet Protocol address,
- characteristics of protected classifications such as minority status or handicaps,
- biometric information,
- geolocation information,
- employment and educational information,
- browsing histories and on-line tracking information, and
- "audio, electronic, visual, thermal, olfactory [!] or similar information."

PI also includes any inferences from any of this information used to create a *profile* reflecting the consumer's preferences, characteristics, and the like. In short, it includes virtually all information an enterprise might collect regarding its customers and potential customers.

Information that is publicly available from government databases is excluded from PI but *only* to the extent that it is used for purposes that are "compatible with" the purposes for which the government agency collected and makes available the information.

Obligations of Entities Subject to the CCPA

If your company is covered (and you almost certainly are) and the information you collect is within the CCPA's scope (it almost certainly is), what must you do to comply? The requirements are detailed, of course, but fall into several key areas:

- **Disclosure.** Upon receipt of a verifiable consumer request, the business must disclose to the consumer the categories *and specific pieces* of PI the business has collected regarding that consumer. The business must also, on request, disclose the types of sources it uses to collect the information, the purpose of such collection, and the categories of third parties with whom it shares such information.

- **Access.** The CCPA prescribes specific procedures that businesses must follow to give consumers access to the PI they have collected. For example, the business must provide *at least* two means of requesting the information, including a toll-free number and a website address if the business has one.

- **Advance Notice.** At or before collection of PI (and without the requirement for a consumer request), the business must inform the consumer as to the categories of PI it is collecting and the purposes for which it will use that information.

- **Deletion.** Upon request by a consumer, the business must delete the consumer's PI from its records and direct all its service providers to do so as well within 45 days of a consumer's request. The business may, however, retain information that is necessary for it to perform certain specified functions.

- **Do-Not-Sell (Opt-Out).** Consumers have the right at any time to demand that the business cease selling their PI until the consumer expressly authorizes the recommencement of such sales. This is true not only for the business that originally collects the information but for any business to which the first business sells the information which then desires to resell the information. Both must expressly alert the consumer of such sale and their opt-out rights.

- **Non-Discrimination.** The business may not discriminate against consumers who exercise their rights under the CCPA, though it may offer financial incentives or payments for sharing PI.

The CCPA also requires companies to inform consumers of their rights, to make specific disclosures pro-actively on their websites, and to follow specific technical requirements regarding the manner of disclosure, means for allowing consumers to make requests, and procedures for processing such requests. There are also a number of narrow exceptions and permitted uses spelled out in the Act.

How the CCPA Will Affect your Telecom and IT Agreements

The CCPA will impact your relationships with telecom and IT providers in several ways, and we recommend that you get ahead of the curve by amending those agreements now so that you will be in compliance by January 1, 2020. First, the CCPA requires a business that has received a consumer request to delete the consumer's PI not only to delete the PI within its own possession but to direct its service providers to delete that PI as well. This means that each of your service providers, telecom or otherwise, that collects or stores your customers' PI will have to comply with that request within 45 days.

That will also mean that they will have to store any of your customers' PI in their possession in a manner that will enable them to sort it by individual so that it can be selectively deleted without disturbing other PI. In our experience, it is unwise to assume that your service providers will be willing and able to comply with such requests; better to force the issue now and demand contractual language that will allow you to pull the trigger and get the required results if and when a consumer invokes his or her rights.

Second, if you are relying on any service provider to keep the primary (or your only backup) copy of any such PI, you will need to add provisions to your agreement with that provider that require it to produce PI in the manner prescribed so that you can turn it over to the requesting consumer within the 45-day timeframe in a format that complies with the Act. You will also want to prohibit your service providers from creating profiles from PI, or at least restrict their ability to do so to narrowly defined instances, so that you can disclose these to the affected consumers. Finally, you'll want to add a specific provision that your service provider will comply with the CCPA and reasonably cooperate with your efforts to comply with the Act.

Enforcement

The CCPA authorizes the California Attorney General to enforce the law via civil action, with fines up to $2500 per violation ($7500 if intentional), where violations are not cured within 30 days of notice. The CCPA also gives consumers whose PI is subject to unauthorized access a private right of action to recover either their actual damages or, if greater, statutory damages of up to $750 *per incident*; this right too is subject to a 30-day notice and cure provision. Injunctive relief is also available.

Disclaimer & For More Information

The above is merely a summary and doesn't get into the deeper details. It isn't legal advice. A careful analysis of the ways in which your company and its specific practices and service provider agreements are impacted by CCPA is imperative to avoid potentially large exposure.

For further information, please contact Kevin DiLallo (kdilallo@lb3law.com) or Patrick Whittle (pwhittle@lb3law.com), or the LB3 lawyer or TC2 consultant with whom you regularly work.