July 11, 2018
Special Edition

Skadden

Privacy & Cybersecurity Update

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Four Times Square
New York, NY 10036
212.735.3000

California Enacts Sweeping New Privacy Law

On June 28, 2018, California Gov. Jerry Brown signed into law the California Consumer Privacy Act (CCPA or "the Act"), which is the broadest and most comprehensive privacy law enacted in the United States to date.[1] The CCPA will affect any organization collecting or storing data about California residents and may effectively set the floor for nationwide privacy protection, since organizations may not want to maintain two privacy frameworks — one for California residents and one for all other citizens. In general, the CCPA will give consumers more information and control over how their data is being used and requires companies to be more transparent in their handling of personal information.

Importantly, the CCPA does not go into effect until January 1, 2020. As discussed below, the California legislature passed CCPA fairly quickly to avert a proposed California ballot initiative in November 2018 that sought to impose even more stringent privacy regulations. Some have argued that the rush to pre-empt the November ballot left CCPA with ambiguities that will need to be resolved over time and that the Act, as currently drafted, may not be the final law that goes into effect.

California has frequently been at the forefront of privacy regulation in the United States. In 2002, California was the first state to enact a security breach notification law, which became a model for similar laws passed by a number of other states. Similarly, in 2015, the state passed the California Online Privacy Protection Act (COPPA) and the Electronic Communications Privacy Act (ECPA).[2] As with the security breach notification law, these two laws have served as model regulations emulated by other states.

[1] The text of the CCPA is available here.

[2] COPPA applies to an operator of a commercial website, online service or mobile application that collects personally identifiable information through the internet about individual consumers residing in California who use or visit its commercial website or online service. The ECPA strictly limits the ability of government authorities to seek electronic information for law enforcement purposes.

Overview of the Law

The intent of the CCPA is to provide California consumers the right to: (1) know what personal information is being collected about them; (2) know whether their personal information is sold or disclosed and to whom; (3) prohibit the sale of their personal information; (4) access their personal information; and (5) receive equal service and price, even if they exercise their privacy rights.

Effective Date of the CCPA

The CCPA will not become effective until January 1, 2020. Until that time, the California attorney general will be responsible for issuing a number of different regulations and interpretations of the law. In addition, the California legislature is likely to pass a variety of technical corrections and clarifications of the law to address issues and ambiguities that have been raised by consumers and businesses.

Businesses and Information Subject to the Law

Covered Business Entities

The CCPA applies to entities that conduct business in California that either directly or indirectly control personal information collection, or that control or are controlled by such an entity and share common branding, and that meet one or more of the following criteria:

- Have annual gross revenues in excess of $25 million, adjusted for inflation;
- Derive 50 percent or more of their annual revenues from selling consumers' personal information; or
- Annually buy, receive for a commercial purpose, sell or share the personal information of 50,000 or more consumers, households or devices.

For the purposes of this summary, we refer to these as "Business Entities."

Information Subject to the Law

The CCPA defines personal information broadly — far more broadly than, for example, various state laws on data breach notification. Under the CCPA, 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." The law goes on to give a number of different examples of personal information that is subject to the law, including:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number or other similar identifiers;
- Information about a consumer's physical characteristics or descriptions, education or any other financial, medical or health insurance information. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records;
- Commercial information, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including browsing history, search history and information regarding a consumer's interaction with an internet website, application or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory or similar information;
- Professional or employment-related information;
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act; and
- Inferences drawn from any of the above information to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.

Publicly available information is excepted from this definition, but that term is narrowly defined and appears to be limited to information that is available through government offices and not, for example, online through private services.

Personal information is not limited to information relating to a consumer but includes that relating to a "household" and thus could include such data as utility usage or delivery history. Further, despite the apparent narrowness of the term, the law does not limit a "consumer" to a purchaser of products or services but rather defines it to include any resident of California, whether or not there is any business relationship between the company and the individual or household.

The CCPA does not, however, apply to personal information subject to the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, or to medical information governed by California's Confidentiality of Medical Information Act or the rules established under the Health Insurance Portability and Accountability Act (HIPAA).

Obligations for Business Entities Under CCPA

Disclosure

The CCPA requires Business Entities to disclose, upon request from a consumer, a significant amount of information about that consumer's personal information, specifically:

- The categories and particular pieces of personal information that are collected, sold or disclosed about a consumer;
- The categories of sources from which that information is collected;
- The business purposes for collecting or selling that information; and
- The categories of third parties with which the information is shared.

The request must be a "verifiable consumer request" — a request made by the consumer or a representative of the consumer that can be reasonably verified by the Business Entity. The California attorney general is to promulgate regulations as to what is a verifiable consumer request.

In addition to responding to these specific requests, Business Entities must also make some information generally available. Specifically, they must make an online disclosure — including in their general privacy policy or any California-specific description of privacy rights — of certain information about the CCPA, including: (1) a description of the consumer's rights under the Act; and (2) a list of categories of personal information collected, sold to a third party or disclosed for business purposes. Business Entities must update this disclosure at least annually.

Access and Portability

The CCPA allows consumers the right to access a copy of the specific pieces of personal information that a Business Entity has collected about that consumer. The Business Entity is to deliver this information "in a readily useable format that allows the consumer to transmit [the] information from one entity to another entity without hindrance." In effect, this requirement gives consumers a data portability right since they can migrate their personal information from one service provider to another offering similar services.

The CCPA requires Business Entities to provide two or more designated methods to request a copy of this information. At a minimum, these must include a toll-free number and, if the business has a website, a website address.

Deletion Requests

Beyond disclosure, Business Entities must also honor a consumer's verified request to delete their personal information. In honoring this request, the Business Entity must also direct service providers to delete information held on the Business Entity's behalf. Business Entities may only refuse to delete such information under certain defined circumstances, some of which are relatively clear and some of which are not. Specifically, Business Entities may refuse to delete information if retaining the information is necessary in order to:

- Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer;
- Detect security incidents, protect against malicious, deceptive, fraudulent or illegal activity, or prosecute those responsible for that activity;
- Conduct debugging to identify and repair errors that impair existing intended functionality;
- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law;
- Comply with the criminal proceeding requirements under the California Electronic Communications Privacy Act pursuant to the California Penal Code;

- Engage in public or peer-reviewed scientific, historical or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the Business Entity's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent;
- Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;
- Comply with a legal obligation; or
- Otherwise use the consumer's personal information internally in a lawful manner that is compatible with the context in which the consumer provided the information.

In addition, if a verified consumer request is "manifestly unfounded or excessive" (including if it is repetitive), a Business Entity may either charge a reasonable fee for the deletion or refuse to act on the request and notify the consumer of the reason for refusing the request.

Right to Opt Out

Business Entities must also provide consumers the right to opt out of the sale of their personal information. This right must be made clear to the consumer through a clear and conspicuous link on the Business Entity's homepage titled "Do Not Sell My Personal Information," as well as a link to the relevant privacy policies. Business Entities, under the CCPA, must respect a consumer's decision to opt out of the sale of their personal information for at least 12 months before requesting the consumer to reauthorize the sale of personal information. The CCPA provides for additional regulations for personal information of children under the age of 16, including a requirement that they (or their parent for children under 13) affirmatively opt in to the sale of their information.

No Discrimination

The CCPA forbids Business Entities from discriminating against consumers with respect to prices, scope of services or denial of services based on the consumer's exercise of his or her rights under the CCPA. There are, however, some key exceptions to this prohibition that seem to undermine the prohibition itself.

First, the Business Entity may charge different prices or provide a different level of service if the difference is "reasonably related to the value provided to the consumer by the consumer's data."

Second, the Business Entity may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information or the deletion of personal information. It may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data. In either of these cases, the consumer must affirmatively opt in to these financial incentives, after receiving a notice that meets certain specific requirements.

Operational Changes

The CCPA also requires Business Entities to provide a privacy policy, which it must update at least every 12 months, describing:

- The consumer's rights under the CCPA, together with one or more methods for submitting requests;
- A list of the categories of personal information it has collected about consumers in the preceding 12 months;
- A list of the categories of personal information it has sold about consumers in the preceding 12 months; and
- A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months.

Business Entities must ensure that all individuals who are responsible for handling consumer inquiries about their privacy practices or compliance are informed of the Business Entity's obligations and how to direct consumers to exercise their rights under the CCPA.

Enforcement

With the exception of when there is a data breach (as discussed below), the CCPA does not provide for a private right of action. Instead, enforcement is by the California attorney general. Business Entities that do not cure a violation within 30 days of notice from the attorney general are subject to the following statutory damages:

- Damages of up to $2,500 per violation for those violation(s) in which a Business Entity did not cure within the 30-day window; and/or
- Damages of up to $7,500 per violation for those intentional violation(s) of the CCPA.

Note that it is not clear from the CCPA itself whether "per violation" means per record or per incident, so it is not clear whether a single incident involving 100 records would be subject to, for example, $2,500 in liability or $250,000 in liability. There is some evidence that the legislature intended the latter (specifically, in the Senate Floor Analysis, which refers to damages being applied per consumer per incident), but it is not conclusive.[3]

Consumers have a potential civil right of action against Business Entities if there has been unauthorized access and exfiltration, theft or disclosure of certain categories of nonencrypted or nonredacted personal information due to failure to implement reasonable security procedures and practices. Consumers may institute a civil action to do any of the following:

- Recover damages in amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater;
- Obtain injunctive or declaratory relief; or
- Obtain any other relief the court deems proper.

If a consumer wishes to bring a private claim or class action for statutory damages, they must provide the Business Entity with 30 days' written notice. If the Business Entity cures the breach within 30 days, it can avoid those damages. This notice is not required for a claim of actual damages. If the Business Entity does not cure the breach, consumers must notify the California attorney general, who must do one of the following within 30 days:

- Notify the consumer of the attorney general's intent to prosecute the violation (if the attorney general does not prosecute within six months, the consumer may proceed with the action);
- Refrain from bringing an action (in which case the consumer can proceed immediately); or
- Notify the consumer(s) that they may not proceed with the action.

It is not clear from the CCPA itself whether a decision by the attorney general to proceed with an action precludes the consumer from bringing a separate action, but that was likely the Act's intent.

[3] The Senate Floor Analysis is available here.

In the context of security breaches, personal information is defined more narrowly than for other provisions of the Act. For purposes of security breach provisions, personal information means a consumer's first name or first initial and his or her last name and one of the following:

- Social Security number;
- Driver's license number or California identification card number;
- Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account;
- Medical information; or
- Health insurance information.

It is not clear from the CCPA itself whether this right of action is intended to be limited to the typical security breach that is the subject of various data breach notification statutes. Conceivably, this right of action applies to more general failure to follow the Act's requirements for notification and consent prior to a sale of personal information, or for deletion of personal information if that information is later made available to employees or third parties.

The CCPA also makes it far easier for consumers to sustain a data breach claim under the Act by not requiring that consumers make a showing of harm from the incident. The inability of consumers to establish any harm has, to date, resulted in the dismissal of many data breach cases for lack of standing.

Comparison With the GDPR

Many companies have recently completed internal revisions to their policies and procedures in order to comply with the European Union's General Data Protection Regulation (GDPR), which took effect in May 2018. Now faced with the CCPA, many wonder whether compliance with GDPR will largely also satisfy compliance with the CCPA. Unfortunately, while there are some broad similarities between the two laws, compliance with one is not likely to result in compliance with the other.

Similar to the CCPA, the GDPR promises to strengthen data protection and privacy for individuals, and sets forth considerable penalties for companies that fail to comply. The GDPR and the CCPA also both seek to codify certain consumer rights, such as the deletion of personal information and data portability.

However, the CCPA and the GDPR are different in execution and with respect to some specific details:

- The CCPA's definition of personal information is more extensive than that in the GDPR;
- The CCPA includes a variety of specific requirements that are not present in GDPR, such as specific disclosures and the use of certain communication channels (such as toll-free phone numbers);
- The CCPA and GDPR have different approaches to the issue of personal information deletion, including arguably broader rights to request deletion under the CCPA and different exceptions under the two laws;
- The CCPA also includes arguably broader rights to access personal information held by a Business Entity than does the GDPR and does not provide all of the exceptions available under the GDPR; and
- The CCPA includes more stringent restrictions on sharing personal information for commercial purposes than does the GDPR.

Therefore, it is unlikely that compliance with the GDPR will necessarily result in compliance under the CCPA. Business Entities that are GDPR-compliant must carefully consider the particular rights, obligations and exceptions under the CCPA.

Key Takeaway: The Future Is Uncertain

The CCPA could become the most significant privacy law in the United States in terms of the rights offered to consumers and the impact it will have on many businesses. Due at least in part to the rushed circumstances in which it passed, however, it has been criticized for retaining ambiguities that will need to be resolved (such as the status of anonymized information) and for leaving for later some key details. It has also been criticized for the financial impact it will likely have on data-based business, especially if large numbers of consumers take advantage of the rights set forth in the CCPA.

Given that the law is not set to take into effect until January 1, 2020, it is likely the California Legislature may consider amendments in the coming months. In addition, the California attorney general has been tasked with developing some of the law's more detailed requirements. Barring a fundamental revision to the law, however, the CCPA will require many businesses to significantly alter their policies and procedures with respect to how they handle personal information. As many companies learned when taking steps to comply with the GDPR, this can be a time-consuming process. In the coming weeks, companies should start proactively evaluating their privacy compliance programs and sketch out a road map for CCPA compliance by 2020.