Client Alert
September 26, 2018

California Consumer Privacy Act

California Adopts Major Changes to Data Privacy Laws

by Daniel Appelman & Michael Plumleigh

In June, 2018, California's legislature enacted sweeping changes to the state's data privacy laws. The California Consumer Privacy Act ("CCPA") amends California's Civil Code to give California consumers new rights in their personal data; and it significantly expands compliance requirements in how businesses collect, use, share and protect that data.[1]

The CCPA is a complex piece of legislation, the most far-reaching consumer privacy and data protection law in the United States. The new law becomes effective on January 1, 2020; but businesses should begin preparing for it now.

This client alert describes many of the CCPA's new consumer rights and business compliance requirements, but it is not exhaustive. For additional information and guidance, please contact one of the attorneys listed below.

New Consumer Rights

The CCPA gives California consumers the right to be fully informed as to what personal data businesses collect about them, the right to receive copies of their data, the right to opt out of having their data sold, a prohibition on selling the personal data of minors unless those minors opt in, and the right to request the deletion of their data. We have summarized these rights below.

The Right to Know What Personal Information Is Collected, Sold or Disclosed; Obligation to Respond to Consumer Requests

The CCPA prohibits businesses from collecting or using personal information for purposes that are not disclosed in advance to consumers.

The CCPA requires that, before a business collects any personal information from California consumers, it must disclose what statutory categories of personal information it intends to collect[2] and the purposes for which it will use that information. Beginning January 1, 2020 businesses wishing to collect personal data from consumers must provide that information in their privacy policies.

Consumers have the right to request that any business that collects their personal information disclose the statutory categories of the information collected, the categories of sources from which it was collected, the business or commercial purpose for collecting that information, the categories of third parties with whom the business shares that information and the specific pieces of personal information that the business has collected about them.

Consumers also have the right to request that any business that sells or discloses their personal information to others disclose the statutory categories of personal information collected, sold or disclosed and the categories of third parties to whom the personal information was sold or disclosed.

Businesses that receive such consumer requests must reply promptly by mail or electronically, free of charge.

Right to Obtain Copies of Personal Information

The CCPA gives California consumers the right to obtain copies of all personal information that a business has collected about them free of charge. If that information is delivered electronically, it must be portable, allowing the consumer to transmit it to others. Thus by January 1, 2020 businesses must institute procedures that will enable them to comply with consumer requests for copies of their personal information.

Right to Request Deletion of Personal Information

The CCPA gives California consumers the right to

request the deletion of their personal information that businesses have collected. Businesses must inform consumers of that right in their privacy policies, and businesses that receive such requests must delete the consumers' personal information from their records and direct any service providers to delete that information from their records as well.[3]

Right to Opt Out of the Sale of Personal Information

Under the CCPA, California consumers have the right to prohibit any business that collects personal information from selling that information to others. Businesses intending to sell consumers' personal information to third parties are required to provide notice to those consumers of such intent and to inform them of their opt out rights.

The CCPA requires all businesses to provide clear and conspicuous links for opting out on their Internet homepages and also in their privacy policies titled "Do Not Sell My Personal Information." Those links must bring consumers to a web page that enables them to opt out of the sale of their personal data. Businesses that have received direction from a consumer not to sell their personal information are prohibited from doing so.

Third parties that buy consumer personal information from a business are prohibited from selling that information unless the consumer has received explicit prior notice of the sale and is provided an opportunity to exercise his or her right to opt out.

Note that these opt out rights will raise complex issues in merger and acquisition transactions.

Minors' Opt In Right

The CCPA prohibits businesses from selling the personal information of California consumers under sixteen years of age[4] unless the consumer expressly authorizes the sale. This prohibition is triggered if a business has actual knowledge that the consumer is less than sixteen years old. A business that willfully disregards the consumer's age is deemed to have had actual knowledge of the consumer's age.

Expanded Definition of "Personal Information"

Current California law protects certain limited categories of personal data. The CCPA expands the kinds of personal data that are legally protected. The new law's definition of "personal information" includes not only demographic identifiers but also (i) online identifiers including aliases, internet protocol address, online or mobile account identifiers and email address, (ii) commercial information, including records of personal property, products or services purchased, obtained or considered, and other purchasing or consuming histories or tendencies, (iii) biometric information, (iv) Internet or other electronic network activity information, including browsing history, search history and information relating to a consumer's interaction with Internet websites, apps and advertisements, (v) consumers' geolocation data, (vi) audio, electronic, visual, thermal, olfactory or similar information, (vii) professional or employment-related information, (viii) educational information that is not publicly available, and (ix) inferences drawn from any of the foregoing that are used to create profiles reflecting consumer preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.

Complying With the CCPA

New Privacy Policy Requirements

Current California law requires every company that collects personal information from consumers online to post a privacy policy that discloses what information it collects, how it uses that information and with whom it shares that information. The CCPA's new provisions require every business that collects personal information from California consumers, online or not, to revise its privacy policies and update them at least once a year.

In order to comply with the CCPA, privacy policies must include a disclosure of the new rights described in this

For more information on privacy law, please contact :

Daniel Appelman
650.331.7014 /dappelman@mh-llp.com
or
Michael Plumleigh
650.331.7005/mplumleigh@mh-llp.com

Client Alert, identify one or more methods for submitting the requests permitted by the new law, and itemize separate lists of the categories of personal information the business has collected, sold and disclosed about consumers.

Duty to Respond to Consumer Requests

Businesses receiving requests from California consumers regarding their personal information must respond to those requests within 45 days of receipt, although an extension of time is possible under some circumstances. It also requires such businesses to make available to consumers at least two designated methods for submitting requests, including a toll-free telephone number and a website address.

Although the CCPA does not become effective until January 1, 2020, we recommend that businesses take steps to comply with it now, as the law is likely to have some retroactive effect. For example, the CCPA's mandatory disclosure provisions require companies to inform consumers of the personal information they've collected, sold or disclosed looking back twelve months from the date of the consumer's request. Thus, any business receiving a consumer request in January, 2020 would be required to disclose all personal information it collected, sold or disclosed looking back to January, 2019. This may be difficult to do unless the business has implemented a data inventory that can identify the personal information of requesting consumers that the business collected, sold and/or shared in 2019.

Prohibition Against Discrimination

The CCPA prohibits businesses from discriminating against consumers who exercise any of their rights under the new law. The prohibition against discrimination includes bans on denying goods or services or providing different levels or qualities of goods or services to consumers who exercise the rights given to them in the CCPA. However, the CCPA permits businesses to offer financial incentives, including payments, as compensation for allowing them to collect, use and sell their personal information.

Mandatory Data Security Measures

Current California guidelines require businesses to disclose the measures they employ to protect consumers' personal information from unauthorized access or disclosure. The CCPA goes further. It requires businesses to take reasonable measures to protect the personal information they collect. Reasonable measures include encrypting or redacting that information. The CCPA gives consumers who have been damaged by a business's failure to take reasonable security measures, and the California Attorney General, the right to sue for civil damages. See *Enforcement* below for the remedies available in such a lawsuit.

Who Is Protected

The CCPA protects consumers. But its definition of "consumer" is unusually broad. It includes anyone who is a California resident. This includes not just the customary understanding of "consumers" but also employees, individuals associated with commercial customers, independent contractors, and visitors to company premises. Thus, even if your business does not market to consumers as traditionally understood, it must comply with the CCPA if it collects any personal information from ANY individual who is a California resident, including your employees, independent contractors or other third parties.

The CCPA protects consumers who are California residents; but most companies doing business nationally or internationally will find it impractical to implement two different sets of compliance procedures, one for California residents and the other for consumers elsewhere. Therefore, as a practical matter, the CCPA will protect all consumers regardless of where they reside.

To some extent, U.S. businesses already face a similar decision whether to base their compliance practices on the requirements of the European Union's General Data Protection Regulation (GDPR), regardless of where in the world the consumers from whom they collect data reside, or to implement two or more different compliance procedures, one for residents of the EU and others for residents of other countries.[5] See *The CCPA and the GDPR*, below.

In response, a number of Internet companies have begun

lobbying Congress to enact national privacy legislation that would preempt the CCPA and would be less restrictive.[6]

Who Must Comply

Every business that collects personal information from California residents and meets one of the following criteria must comply with the CCPA: (i) annual gross revenues over $25 million; (ii) the business buys, receives, sells or shares the personal information of more than 50,000 California consumers for commercial purposes; or (iii) more than 50% of the business's income comes from selling personal information belonging to California residents.

Companies worldwide that meet one of the foregoing criteria must comply with the CCPA unless they can show that they do not engage in any commercial conduct in California or with California consumers. Most U.S. companies will find it difficult to do so.

Exclusions

The CCPA does not apply to the collection or sale of personal information that takes place completely outside of California regarding the personal information of non-California consumers.

The CCPA excludes data that are already protected by certain existing California or federal laws, including confidential medical information covered by the California Confidentiality of Medical Information Act, the federal Health Insurance Portability and Availability Act and the financial data covered by the Gramm-Leach-Bliley Act. However, any personal medical or financial data not covered by those laws are covered by the CCPA.

Enforcement

The CCPA gives consumers a private right of action in the event that a business's violation of its duty to implement and maintain reasonable security procedures and practices results in unauthorized access, theft or disclosure of a consumer's sensitive personal information.[7] Remedies in a civil lawsuit may include the recovery of actual or statutory damages, whichever is greater. The CCPA provides for statutory damages up to $750 per consumer per incident. However, no action for statutory damages is permitted unless the consumer provides the business with thirty (30) days prior written notice of the violations and the business fails to cure those violations within that period. There is no advance notice requirement in the CCPA for a consumer action that seeks actual damages. The CCPA also permits courts to grant injunctive or declaratory relief and any other relief that the courts deem proper.

The CCPA's private right of action only applies to violations that constitute security incidents.[8] However, the California Attorney General can sue businesses for any violation of the CCPA if they fail to cure the violation within 30 days after being notified. Liability to the State of California for noncompliance with the CCPA can be up to $2,500 for each violation, or up to $7,500 per violation if noncompliance is intentional. The proceeds of any successful lawsuit brought by the Attorney General will be deposited in a special account known as the Consumer Privacy Fund. The legislature can use the proceeds in that account to offset any costs incurred by the Attorney General and the courts in bringing and hearing the lawsuits.

Regulation and Implementation

The CCPA requires the California Attorney General to solicit public input and to adopt regulations to interpret and clarify the new law, update additional categories of personal information covered, and facilitate its implementation as changes in technology, data collection and consumer expectations become evident. The Attorney General may not bring an enforcement action for violation of the CCPA until six months after it publishes the new regulations or July 1, 2020, whichever occurs first.

The CCPA and the GDPR

The CCPA and the GDPR both grant consumers extensive new rights to control the use of, and to protect, their personal information; and both impose on businesses significant new compliance requirements. However, the scope and particularities of the two laws vary considerably. Complying with the CCPA does not ensure that a business is in compliance with the GDPR, and vice versa.

Recommendations

The CCPA contains many ambiguities that will have to be clarified by amendment, regulatory interpretation and judicial rulings. In the short term, we advise clients to begin implementing procedures to comply with the CCPA's new requirements so they will be ready when it becomes effective on January 1, 2020. At a minimum, these should include:

- updating your company's privacy policy to inform consumers of their new rights, and then further updating the privacy policy at least once a year thereafter;
- providing links on the company's Internet homepage and also in its privacy policies titled "Do Not Sell My Personal Information" for opting out;
- providing consumers with at least two ways to submit information requests, including a toll-free number and a website address;
- implementing procedures for responding to consumer requests to access their personal information, to receive copies of that information, to disclose the statutory categories of information collected and sold, to opt out of having that information sold and to delete that information;
- implementing procedures to determine whether a consumer is under sixteen years old, and to refrain from selling such consumer's personal information unless the consumer, or his or her parent, has affirmatively opted in to that sale;
- creating or updating a data inventory that can be used to track the company's data processing activities, consumer requests and the company's responses to those requests;
- if your company uses third parties to process the personal information you collect, reviewing and updating the contracts with those third parties to prohibit them from retaining, using, or disclosing the PI for any purpose other than for the specific purpose of performing the services specified in the contract;
- training employees who handle consumer requests on the relevant policies and procedures to ensure that they are able to comply with those requests expeditiously; and
- considering encrypting or redacting the personal information you collect to minimize the possibility of a civil lawsuit for violating the CCPA's requirement to implement reasonable security measures.

[1] AB 375, California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended by SB 1121.

[2] The required categorization is set forth in Cal. Civ. Code § 1798.140(o)(1).

[3] The CCPA includes a number of exceptions to this requirement that are beyond the scope of this client alert.

[4] Presumably this is as of the date of sale, but the CCPA is not clear on this point.

[5] The General Data Protection Regulation became effective in May of this year.

[6] *See, e.g.,* Cecilia Kang, *"Tech Industry Pursues a Federal Privacy Law, on Its Own Terms,"* New York Times, August 26, 2018.

[7] Cal. Civ. Code § 1798.81.5(d)(1)(A) lists a subset of the broad definition of personal information, the unauthorized access, theft or disclosure of which could subject a business to civil action. Lawsuits by the California Attorney General for violations of other parts of the CCPA can use the broader definition.

[8] Cal Civ. Code § 1798.150(a).

M&H, LLP
525 Middlefield Road, Suite 250
Menlo Park, California 94025
650.331.7000
www.mh-llp.com