GIBSON DUNN

July 12, 2018

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

To Our Clients and Friends:

On June 28, 2018, Governor Jerry Brown signed the California Consumer Privacy Act of 2018 ("CCPA"), which has been described as a landmark privacy bill that aims to give California consumers increased transparency and control over how companies use and share their personal information. The law will be enacted as several new sections of the California Civil Code (sections 1798.100 to 1798.198). While lawmakers and others are already discussing amending the law prior to its January 1, 2020 effective date, as passed the law would require businesses collecting information about California consumers to:

1. disclose what personal information is collected about a consumer and the purposes for which that personal information is used;

2. delete a consumer's personal information if requested to do so, unless it is necessary for the business to maintain that information for certain purposes;

3. disclose what personal information is sold or shared for a business purpose, and to whom;

4. stop selling a consumer's information if requested to do so (the "right to opt out"), unless the consumer is under 16 years of age, in which case the business is required to obtain affirmative authorization to sell the consumer's data (the "right to opt in"); and

5. not discriminate against a consumer for exercising any of the aforementioned rights, including by denying goods or services, charging different prices, or providing a different level or quality of goods or services, subject to certain exceptions.

The CCPA also empowers the California Attorney General to adopt regulations to further the statute's purposes, and to solicit "broad public participation" before the law goes into effect.[1] In addition, the law permits businesses to seek the opinion of the Attorney General for guidance on how to comply with its provisions.

The CCPA does not appear to create any private rights of action, with one notable exception: the CCPA expands California's data security laws by providing, in certain cases, a private right of action to consumers "whose nonencrypted or nonredacted personal information" is subject to a breach "as a result of the business' violation of the duty to implement and maintain reasonable security procedures," which permits consumers to seek statutory damages of $100 to $750 per incident.[2] The other rights embodied in the CCPA may be enforced only by the Attorney General—who may seek civil penalties up to $7,500 per violation.

In the eighteen months ahead, businesses that collect personal information about California consumers will need to carefully assess their data privacy and disclosure practices and procedures to ensure they are in compliance when the law goes into effect on January 1, 2020. Businesses may also want to consider whether to submit information to the Attorney General regarding the development of implementing regulations prior to the effective date.

I. Background and Context

The CCPA was passed quickly in order to block a similar privacy initiative from appearing on election ballots in November. The ballot initiative had obtained enough signatures to be presented to voters, but its backers agreed to abandon it if lawmakers passed a comparable bill. The ballot initiative, if enacted, could not easily be amended by the legislature,[3] so legislators quickly drafted and unanimously passed AB 375 before the June 28 deadline to withdraw items from the ballot. While not as strict as the EU's new General Data Protection Regulation (GDPR), the CCPA is more stringent than most existing privacy laws in the United States.

II. Who Must Comply With The CCPA?

The CCPA applies to any "business," including any for-profit entity that collects consumers' personal information, which does business in California, and which satisfies one or more of the following thresholds:

A. has annual gross revenues in excess of twenty-five million dollars ($25,000,000);

B. possesses the personal information of 50,000 or more consumers, households, or devices; or

C. earns more than half of its annual revenue from selling consumers' personal information.[4]

The CCPA also applies to any entity that controls or is controlled by such a business and shares common branding with the business.[5]

The definition of "Personal Information" under the CCPA is extremely broad and includes things not considered "Personal Information" under other U.S. privacy laws, like location data, purchasing or consuming histories, browsing history, and inferences drawn from any of the consumer information.[6] As a result of the breadth of these definitions, the CCPA likely will apply to hundreds of thousands of companies, both inside and outside of California.

III. CCPA's Key Rights And Provisions

The stated goal of the CCPA is to ensure the following rights of Californians: (1) to know what personal information is being collected about them; (2) to know whether their personal information is sold or disclosed and to whom; (3) to say no to the sale of personal information; (4) to access their personal information; and (5) to equal service and price, even if they exercise their privacy rights.[7] The CCPA purports to enforce these rights by imposing several obligations on covered businesses, as discussed in more detail below.

A. Transparency In The Collection Of Personal Information

The CCPA requires disclosure of information about how a business collects and uses personal information, and also gives consumers the right to request certain additional information about what data is collected about them.[8] Specifically, a consumer has the right to request that a business disclose:

1. the categories of personal information it has collected about that consumer;

2. the categories of sources from which the personal information is collected;

3. the business or commercial purpose for collecting or selling personal information;

4. the categories of third parties with whom the business shares personal information; and

5. the specific pieces of personal information it has collected about that consumer.[9]

While categories (1)-(4) are fairly general, category (5) requires very detailed information about a consumer, and businesses will need to develop a mechanism for providing this type of information.

Under the CCPA, businesses also must affirmatively disclose certain information "at or before the point of collection," and cannot collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice.[10] Specifically, businesses must disclose in their online privacy policies and in any California-specific description of a consumer's rights a list of the categories of personal information they have collected about consumers in the preceding 12 months by reference to the enumerated categories (1)-(5), above.[11]

Businesses must provide consumers with at least two methods for submitting requests for information, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.[12]

B. Deletion Of Personal Information

The CCPA also gives consumers a right to request that businesses delete personal information about them. Upon receipt of a "verifiable request" from a consumer, a business must delete the consumer's personal information and direct any service providers to do the same. There are exceptions to this deletion rule when "it is necessary for the business or service provider to maintain the consumer's personal information" for one of nine enumerated reasons:

1. 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's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

3. Debug to identify and repair errors that impair existing intended functionality.

4. 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.

5. Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

6. 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 businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

7. To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

8. Comply with a legal obligation.

9. 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.[13]

Because these exceptions are so broad, especially given the catch-all provision in category (9), it is unclear whether the CCPA's right to deletion will substantially alter a business's obligations as a practical matter.

C. Disclosure Of Personal Information Sold Or Shared For A Business Purpose

The CCPA also requires businesses to disclose what personal information is sold or disclosed for a business purpose, and to whom.[14] The disclosure of certain information is only required upon receipt of a "verifiable consumer request."[15] Specifically, a consumer has the right to request that a business disclose:

1. The categories of personal information that the business collected about the consumer;

2. The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold; and

3. The categories of personal information that the business disclosed about the consumer for a business purpose.[16]

A business must also affirmatively disclose (including in its online privacy policy and in any California-specific description of consumer's rights):

1. The category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact; and

2. The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.[17]

This information must be disclosed in two separate lists, each listing the categories of personal information it has sold about consumers in the preceding 12 months that fall into categories (1) and (2), above.[18]

D. Right To Opt-Out Of Sale Of Personal Information

The CCPA also requires businesses to stop selling a consumer's personal information if requested to do so by the consumer ("opt-out"). In addition, consumers under the age of 16 must affirmatively opt-in to allow selling of personal information, and parental consent is required for consumers under the age of 13.[19] Businesses must provide notice to consumers that their information may be sold and that consumers have the right to opt out of the sale. In order to comply with the notice requirement, businesses must include a link titled "Do Not Sell My Personal Information" on their homepage and in their privacy policy.[20]

E. Prohibition Against Discrimination For Exercising Rights

The CCPA prohibits a business from discriminating against a consumer for exercising any of their rights in the CCPA, including by denying goods or services, charging different prices, or providing a different level or quality of goods or services. There are exceptions, however, if the difference in price or level or quality of goods or services "is reasonably related to the value provided to the consumer by the consumer's data." For example, while the language of the statute is not entirely clear, a business may be allowed to charge those users who do not allow the sale of their data while providing the service for free to users who do allow the sale of their data—as long as the amount charged is reasonably related to the value to the business of that consumer's data. A business may also offer financial incentives for the collection of personal information, as long as the incentives are not "unjust, unreasonable, coercive, or usurious" and the business notifies the consumer of the incentives and the consumer gives prior opt-in consent.

F. Data Breach Provisions

The CCPA provides a private right of action to consumers "whose nonencrypted or nonredacted personal information" is subject to a breach "as a result of the business' violation of the duty to implement and maintain reasonable security procedures."[21] Under the CCPA, a consumer may seek statutory damages of $100 to $750 per incident or actual damages, whichever is greater.[22] Notably, the meaning of "personal information" under this provision is the same as it is in California's existing data breach law, rather than the broad definition used in the remainder of the CCPA.[23] Consumers bringing a private action under this section must first provide written notice to the business of the alleged violations (and allow the business an opportunity to cure the violations), and must notify the Attorney General and

give the Attorney General an opportunity to prosecute.[24] Notice is not required for an "action solely for actual pecuniary damages suffered as a result of the alleged violations."[25]

IV. Potential Liability

Section 1798.150, regarding liability for data breaches, is the only provision in the CCPA expressly allowing a private right of action. The damages available for such a civil suit are limited to the greater of (1) between $100 and $750 per consumer per incident, or (2) actual damages. Individual consumers' claims also can potentially be aggregated in a class action.

The other rights embodied in the CCPA may be enforced only by the Attorney General—who may seek civil penalties not to exceed $2,500 for each violation, unless the violation was intentional, in which case the Attorney General can seek up to $7,500 per violation.[26]

---

[1] To be codified at Cal. Civ. Code § 1798.185(a)

[2] Cal. Civ. Code § 1798.150.

[3] By its own terms, the ballot initiative could be amended upon a statute passed by 70% of each house of the Legislature if the amendment furthered the purposes of the act, or by a majority for certain provisions to impose additional privacy restrictions. See The Consumer Right to Privacy Act of 2018 No. 17-0039, Section 5. Otherwise, approved ballot initiatives in California can only be amended with voter approval. California Constitution, Article II, Section 10.

[4] Cal. Civ. Code § 1798.140(c)(1).

[5] Cal. Civ. Code § 1798.140(c)(2).

[6] Cal. Civ. Code § 1798.140(o). The definition of "personal information" does not include publicly available information, and the CCPA also does not generally restrict a business's ability to collect or use deidentified aggregate consumer information. Cal. Civ. Code § 1798.145(a)(5).

[7] Assemb. Bill 375, 2017-2018 Reg. Sess., Ch. 55, Sec. 2 (Cal. 2018)

[8] Cal. Civ. Code § 1798.100 and 1798.110.

[9] Cal. Civ. Code § 1798.110(a).

[10] Cal. Civ. Code §§ 1798.100(b); 1798.110(c).

[11] Cal. Civ. Code §§ 1798.110(c); 1798.130(a)(5)(B).

[12] Cal. Civ. Code § 1798.130(a)(1).

[13] Cal. Civ. Code § 1798.105(d).

[14] Cal. Civ. Code § 1798.115.

[15] Cal. Civ. Code § 1798.115(a)-(b).

[16] Cal. Civ. Code § 1798.115(a).

[17] Cal. Civ. Code § 1798.115(c).

[18] Cal. Civ. Code § 1798.130(a)(5)(C).

[19] Cal. Civ. Code § 1798.120(d).

[20] Cal. Civ. Code § 1798.135.

[21] Cal. Civ. Code § 1798.150.

[22] Cal. Civ. Code § 1798.150.

[23] Cal. Civ. Code § 1798.81.5(d)(1)(A)

[24] Cal. Civ. Code § 1798.150(b).

[25] Cal. Civ. Code § 1798.150 (b)(1).

[26] Cal. Civ. Code § 1798.155.

The following Gibson Dunn lawyers assisted in the preparation of this client alert: Joshua A. Jessen, Benjamin B. Wagner, Christina Chandler Kogan, Abbey A. Barrera, and Alison Watkins.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these issues. For further information, please contact the Gibson Dunn lawyer with whom you usually work or the following leaders and members of the firm's Privacy, Cybersecurity and Consumer Protection practice group:

United States
Alexander H. Southwell - Co-Chair, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
M. Sean Royall - Dallas (+1 214-698-3256, sroyall@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)

Christopher Chorba - Los Angeles (+1 213-229-7396, cchorba@gibsondunn.com)
Richard H. Cunningham - Denver (+1 303-298-5752, rhcunningham@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Shaalu Mehra - Palo Alto (+1 650-849-5282, smehra@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)

Europe
Ahmed Baladi - Co-Chair, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox - London (+44 (0)207071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Bernard Grinspan - Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Jean-Philippe Robé - Paris (+33 (0)1 56 43 13 00, jrobe@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Nicolas Autet - Paris (+33 (0)1 56 43 13 00, nautet@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)
Alejandro Guerrero Perez - Brussels (+32 2 554 7218, aguerreroperez@gibsondunn.com)

Asia
Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)