DrinkerBiddle

Privacy Alert

Rev. October 2019

California Consumer Privacy Act

By Peter Blenkinsop | peter.blenkinsop@dbr.com | +1 202-230-5142

On June 28, 2018, Governor Jerry Brown signed into law the California Consumer Privacy Act of 2018 ("CCPA" or "the Act"). The law was further amended in September 2018 and October 2019. The CCPA takes effect on January 1, 2020, and provides individuals in California with enhanced transparency and control over how companies use and share their personal information. The bill requires the California Attorney General to issue regulations before July 1, 2020 to further specify certain implementation details. The Attorney General issued proposed regulations on October 10, 2019.[1]

BACKGROUND

The CCPA was hastily adopted in late June 2018 as the result of negotiations among stakeholders supporting a California Right to Privacy Act ballot measure and business groups seeking to avoid the ballot initiative. The ballot initiative had secured nearly double the number of California voter signatures necessary to appear on the November 2018 ballot and was widely expected to secure the support of a majority of California voters. Under California law, the California legislature may not amend or repeal an approved ballot measure without submitting the change to voters, unless the measure provides otherwise by its terms. The CA Right to Privacy Act ballot measure included a provision allowing its amendment by a statute securing the support of at least 70% of both houses and signed by the Governor. Recognizing that should the measure be included on the ballot and adopted by voters, it would then be extremely difficult to amend, those opposed to the measure sought to negotiate a compromise in exchange for the withdrawal of the ballot measure by its sponsors. (The deadline in California for withdrawal of ballot initiatives is 131 days before the November general election.) Opponents argued that the ballot measure was overly broad and compliance with it would be extremely onerous. They pointed to the fact that, among other provisions, the ballot measure would have given individuals the right to pursue civil statutory damages of up to $3,000 for each violation of the law, potentially leading to a new wave of class action lawsuits.

OVERVIEW OF REQUIREMENTS

Despite its name, the CCPA applies to a broader class of individuals than colloquial understandings of "consumers." Indeed, the term "consumer" is defined under the Act, in relevant part, as "a natural person who is a California resident." Thus, customers, employees, business contacts, and others are protected individuals under the Act. However, amendments enacted in October 2019 provide a temporary delay in the full application of the CCPA to personal information of employees and certain business contacts. *(See Section F, "Exceptions," below.)*

[1] See our October 2019 Privacy Alert entitled "CCPA Amendments & Proposed Implementing Regulations" for a summary of the Attorney General's proposed regulations.

The requirements of the Act apply to any "business," which is defined to include any for-profit entity that does business in the state of California, determines the purposes and means for the processing of personal information, and (i) has annual gross revenues in excess of $25 million; (ii) possesses the personal information of 50,000 or more consumers, households, or devices; or (iii) earns more than half of its annual revenue from selling consumers' personal information. The definition also includes any entity that controls or is controlled by such a business and that shares common branding with the business.

The CCPA empowers CA residents with the following six data privacy rights vis-à-vis a covered business:

1. *To be provided with information on what personal information is collected about them and the purposes for which that personal information is used;*
2. *To be provided with information on what personal information is sold or disclosed for a business purpose and to whom;*
3. *To opt out of the sale of their personal information to third parties (or in the case of minors under age 16, to require an opt in before the sale of their personal information);*
4. *To request the deletion of their personal information;*
5. *Not to be subject to discrimination for exercising any of the above rights, including by being denied goods or services or being charged a different price, or being subjected to a lower level of quality, of such goods or services; and*
6. *To seek statutory damages of $100 to $750 for breaches of unencrypted personal information that arise as a result of a business's violation of its duty to implement and maintain reasonable security procedures.*

The California Attorney General is authorized to seek civil penalties of up to $7,500 for each violation of the law.

"Personal information" is defined under the CCPA as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" but excludes "publicly available information" that has been lawfully made available from federal, state, or local government records. The Act enumerates eleven categories of personal information:

1. *"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."*
2. *"Any categories of personal information described in subdivision (e) of Section 1798.80." (This list includes the following: name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.)*
3. *"Characteristics of protected classifications under California or federal law."*
4. *"Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies."*
5. *"Biometric information." (This is defined as "an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.")*

6. *"Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement."*
7. *"Geolocation data."*
8. *"Audio, electronic, visual, thermal, olfactory, or similar information."*
9. *"Professional or employment-related information."*
10. *"Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99)."*
11. *"Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."*

A. Transparency and Access Rights

Before or at the time of collecting CA residents' personal information, businesses must, under the CCPA, inform those data subjects of the categories of personal information to be collected (these categories should correspond to the list of eleven categories in the definition of "personal information") and the purposes for which the data will be used. Individuals have the right to request, at any time, information concerning the categories of personal information collected, the categories of sources of the personal information, and any categories of third parties with whom the personal information has or will be shared. Individuals also have the right under the CCPA to request additional information concerning the sale of their personal information and the disclosure of their personal information for business operational purposes.[2] A business receiving such a request must separately identify by category of recipient the categories of personal information sold and disclosed.

Individuals can also request a copy of the personal information held by a business. Businesses must promptly take steps to provide a copy of the personal information in their possession, free-of-charge. The copy must be delivered either by mail or electronically. If the information is provided electronically, it must be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit the information to another

[2] These operational purposes include:

1. Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.
2. Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
3. Debugging to identify and repair errors that impair existing intended functionality.
4. Short-term, transient use, provided the personal information that is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.
5. Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.
6. Undertaking internal research for technological development and demonstration.
7. Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

organization without hindrance. Businesses are not required to provide copies of personal information to data subjects more than twice in a 12-month period.[3]

In order for individuals to exercise their rights above, businesses must make available two or more designated methods for submitting requests, including, at a minimum, a toll-free telephone number and a web site address. The information should ordinarily be provided within 45 days of receiving a request, but if reasonably necessary and notice is provided to the requestor within the initial 45-day period, the period can be extended for an additional 45 days. The information provided must cover at least the 12-month period preceding the business's receipt of the request. There are limited exceptions to the requirement that a business provide the requested information where (i) the business is unable to reasonably verify the requestor's identity, or (ii) the personal information was collected for a one-time transaction and is not further retained. Moreover, the law states that it shall not be construed to require a business to collect any personal information that it would not otherwise collect in the ordinary course of business or retain personal information for longer than it would otherwise retain such information in the ordinary course of business. If a business does not take action on an individual's request, it must inform the individual within the time period allowed of its reasons for not taking any action and of the individual's right to appeal the decision to the business.

In addition, a business must in its online privacy policy, or in a California-specific privacy policy posted on its website, describe CA residents' rights to request the information described above and list the categories of CA residents' personal information it has in the prior 12 months (i) collected, (ii) sold, and (iii) disclosed for business operational purposes.

B. Right to Opt Out of Sale of Personal Information

The CCPA gives CA residents the right to opt out of the sale of their personal information. Upon receipt of an opt-out request, a business must stop selling the information, unless subsequent express authorization is received. The Act has stricter standards with respect to minors. If a business has actual knowledge that a CA resident is under 16 years old, the business must obtain express opt-in before selling the minor's personal information. Minors between 13 and 16 years of age can provide this opt-in themselves. For minors younger than 13 years old, the opt in must be provided by a parent or guardian.

The CCPA provides that "A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age." It is unclear if this language creates an affirmative obligation on the part of businesses to ask CA residents to provide their age when collecting personal information or if this obligation only arises in circumstances in which it would be reasonable to expect that minors may provide personal information (e.g., a website directed towards an audience including minors). It is also unclear if a simple statement at the point of data collection that prohibits minors under 17 from submitting information would be viewed as a sufficient compliance measure.

Under the Act, a "sale" of personal information means "renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information . . . [to] a third party for monetary or other valuable consideration." In legal terms, "valuable consideration" refers to a benefit conferred or a detriment incurred by a party in exchange for a promise by another party. "Valuable consideration" may be non-monetary as long as it is of some value to one or both parties. Thus, a transfer of personal information in exchange for something of value may be considered a "sale" under the CCPA.

[3] A separate exception also exists for requests that "are manifestly unfounded or excessive, in particular because of their repetitive character." Presumably, up to two requests in a 12-month period is, by default, not excessive unless the business can demonstrate otherwise.

Importantly, the definition of a "sale" of personal information excludes (i) a disclosure of personal information at the direction of the individual; (ii) alerting a third-party of an opt-out request; (iii) disclosure of personal information that occurs in the context of a merger, acquisition, bankruptcy, or other transaction, and not as a stand-alone asset, and the recipient assumes the responsibilities of the disclosing party; and (iv) a disclosure to a service provider for a business operational purpose pursuant to a written contract. With respect to disclosures to service providers, the contract must prohibit the service provider from retaining, using, or disclosing the information for any purpose other than for performing the services specified in the contract.

The CCPA stipulates that "[i]f a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title." In a complex transaction in which there are both services being performed and an exchange of personal information, this raises the specter of a disclosure being construed as a "sale," even though the parties have attempted to structure the remuneration as being provided in exchange for the services only.

In addition to describing the right to opt-out in its online privacy policy or California-specific privacy policy, a business must include a "clear and conspicuous" link on its homepage to a web page where individuals can exercise their opt out rights. The link must be titled ""Do Not Sell My Personal Information" and must link to a page with the same title. It is unclear if this link need only be included on the business's corporate web site homepage or also on every site and in every application that the business maintains where personal information is collected. Under the Act, "homepage" is defined as "the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, 'About,' 'Information,' or settings page, and any other location that allows consumers to review [the opt-out notice] including, but not limited to, before downloading the application."

C. Right to Deletion

The CCPA gives CA residents the right to request that a business delete the personal information that the business has collected from that individual. A business must comply with this request unless it is necessary to maintain the information in order to:

1. *Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested or reasonably anticipated by the individual, or otherwise perform a contract with the individual.*
2. *Detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for such activity.*
3. *Identify and repair errors that impair existing intended functionality.*
4. *Exercise free speech or another legal right.*
5. *Comply with a legal obligation.*
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. *Enable solely internal uses that are reasonably aligned with the expectations of the individual based on the individual's relationship with the business.*
8. *Otherwise internally use the individual's personal information in a manner that is compatible with the context in which the individual provided the information.*

It is unclear how these last two exceptions differ and how broadly they will be interpreted. If interpreted broadly, they could significantly narrow the right to deletion. One might surmise that the principle behind these last two exceptions is that when the individual provided the information, he or she may have impliedly waived his or her right in the future to request the deletion of that information. In stark contrast, however, another provision of the CCPA provides that an express waiver of such rights is not allowed: "Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable." This difference in treatment of implied waivers versus express waivers is peculiar, to say the least.

In contrast with the potential breadth of the last two exceptions, the research exception is crafted so narrowly that it is unclear when it would actually be of use. It ostensibly applies to personal information that is needed for "scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws[,] or studies conducted in the public interest in the area of public health." However, the Act stipulates that where personal information that was originally collected for a different purpose is reused for research purposes, the use of the personal information for the research purposes must be compatible with the purpose(s) for which the personal information was originally collected. Further, the personal information:

1. *Must not be used for any commercial purposes. "Commercial purposes" are defined as activities to "advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction."*
2. *Must be "pseudonymized[4] and de-identified,[5] or de-identified and in the aggregate,[6] such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer."*
3. *Must be protected by technical safeguards and business processes that prohibit re-identification of the individuals to whom the information pertains.*
4. *Must be subject to business processes to prevent inadvertent release of de-identified information.*
5. *Must be subject to additional security controls that limit access to the information to only those individuals who require access to carry out the research purposes.*

D. Right Not to Be Subject to Discrimination

Subject to certain important exceptions, the CCPA prohibits a business from discriminating against an individual based on the individual's exercise of his or her rights under the Act. In particular, a business may not deny goods or

---

[4] "Pseudonymize" is defined as "the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer."

[5] "Deidentified" is defined as "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
(2) Has implemented business processes that specifically prohibit reidentification of the information.
(3) Has implemented business processes to prevent inadvertent release of deidentified information.
(4) Makes no attempt to reidentify the information."

[6] "Aggregate consumer information" is defined as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. 'Aggregate consumer information' does not mean one or more individual consumer records that have been de-identified."

services to an individual based on the individual's exercise of his or her rights, nor may a business (i) charge different prices or rates for goods or services, including through the use of discounts, benefits, or imposing penalties; or (ii) provide a different level or quality of goods or services to the consumer, in both cases unless the difference is "reasonably related to the value provided to the business by the consumer's data."

The Act also expressly allows a business to offer financial incentives to individuals, including payments as compensation, for the collection and/or sale of their personal information, provided the financial incentive practices are not "unjust, unreasonable, coercive, or usurious in nature," the material terms of the incentive program have been described to the individual, and the individual has consented to such terms.

E. Private Right of Action in Relation to Data Breaches

The CCPA authorizes California residents whose personal information has been subject to a breach to bring a civil action to recover actual or statutory damages, whichever is greater, where the breach is a result of the business's "violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information." With respect to this section of the law, the definition of "personal information" refers to a section of California's breach notification statute. That statute, as of January 1, 2020, will define "personal information," in relevant part, as: "An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

1. *Social security number.*
2. *Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.*
3. *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.*
4. *Medical information.*
5. *Health insurance information.*
6. *Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes."*

The Act authorizes statutory damages of between $100 and $750 per individual, per incident. In assessing the level of statutory damages, a court can consider all the relevant circumstances, including "the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth."

Before an individual initiates a private action under the CCPA for statutory damages, either on an individual or a class-wide basis, the individual must provide the business with 30 days' written notice identifying the specific provisions of the Act alleged to have been violated or being violated. In the event a cure is possible and the business actually cures the alleged violations within the 30 day period and provides the individual with an express written statement to such effect, the individual is prevented from initiating any claims against the business for statutory damages. If the business violates such representations, the individual may pursue statutory damages for each breach of the express written statement.

In addition to providing notification to the business prior to bringing a civil action, the individual must notify the California Attorney General within 30 days of filing the action. The Attorney General then has 30 days to do one of the following:

1. *To notify the individual that he/she may not bring the civil action;*
2. *To notify the consumer of the Attorney General's intent to bring an action against the business for the violation within a six-month period. If such an action is not brought within the six-month period, the individual may proceed with his/her action; or*
3. *To refrain from taking any action, allowing the individual to proceed with the civil action.*

F. Exceptions

The CCPA includes a number of exceptions. In particular, the Act states that "[t]he obligations imposed on businesses by this title shall not restrict a business's ability to":

1. *"Comply with federal, state, or local laws."*
2. *"Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities."*
3. *"Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law."*
4. *"Exercise or defend legal claims."*
5. *Collect, use, retain, sell, or disclose information that is de-identified or in aggregate form.*
6. *"Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California." Commercial conduct will be viewed as taking place wholly outside of California only if the business collected the information while the individual was outside of California and no part of any sale of the individual's personal information occurred in California or pertains to personal information collected while the individual was in California. A business is not permitted in order to circumvent application of the law to store personal information on a device while the individual is in California and to then retrieve that information when the individual is outside of California.*

In addition, the Act states that, with the exception of the private right of action for data breaches, it does not apply to the following:

1. *Circumstances in which compliance with a requirement of the CCPA would violate an evidentiary privilege under California law.*
2. *An activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, or mode of living by a consumer reporting agency, a furnisher of information for use in a consumer report, or a user of a consumer report.*
3. *The collection, use, and disclosure of personal information pursuant to the Gramm-Leach Bliley Act or the Driver's Privacy Protection Act.*

Moreover, the following types of information are exempt from certain aspects of the law:

1. *Exempt from CCPA provisions concerning the right to opt-out of the sale of personal information: Vehicle information or ownership information retained or shared between a dealer and a vehicle manufacturer, where the information is shared for the purpose of a vehicle repair covered by a warranty or a vehicle recall.*
2. *Exempt through January 1, 2021 from CCPA provisions concerning the right to access, right to delete, and right to opt-out: Personal information collected about an individual acting as a job applicant to, employee of, or contractor to the business.*

3. *Exempt through January 1, 2021 from CCPA provisions concerning the right to transparency, right to access, and right to delete: Personal information collected in the context of a business-to-business relationship, where the personal information reflects a written or verbal communication or a transaction between the business and the individual.*

Finally, there are three separate exceptions that apply to health information. Namely, the Act does not apply to:

1. *"Medical information" governed by the California Confidentiality of Medical Information Act (CMIA) or "protected health information" (PHI) collected by a covered entity or business associate governed by the federal HIPAA regulations.*
2. *A "provider of health care" governed by the CMIA or a covered entity governed by the HIPAA regulations, "to the extent the provider or covered entity maintains patient information in the same manner" as CMIA medical information or HIPAA PHI.*
3. *Information collected as part of a clinical trial subject to the federal Common Rule, pursuant to ICH GCP, or pursuant to FDA human subject protections.*

G. Attorney General Rules and Enforcement

On or before July 1, 2020, the AG must adopt regulations to further elaborate on various aspects of the legislation. As noted previously, the AG issued proposed regulations on October 10, 2019. Businesses are also permitted to seek guidance from the AG on how to comply. The Act states that "A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance." A business that intentionally violates the CCPA can be subject to civil penalties of up to $7,500 for each violation. While the Act goes into effect on January 1, 2020, the Attorney General is not permitted to bring enforcement actions until the earlier of six months after the publication of the final regulations or July 1, 2020.