The Good, Bad, And The Ugly: Key Takeaways From California's New Privacy Law

privacyandcybersecuritylaw.com/the-good-bad-and-the-ugly-key-takeaways-from-californias-new-privacy-law

By Peter Stockburger

Consumer privacy rights in California are well established. The California Constitution expressly grants California citizens a right to privacy. And existing California law provides for the confidentiality of personal information in various contexts, including under the Online Privacy Protection Act, the Privacy Rights for California Minors in the Digital World Act, and Shine the Light. California law also requires businesses that suffer a breach of security to disclose the breach to consumers, and in some instances law enforcement, if sensitive information is compromised.

On June 28, 2018, California governor Jerry Brown further expanded California consumer privacy rights by signing into law the California Consumer Privacy Act of 2018 ("CCPA") (California Civil Code §§ 1798.100 to 1798.198) – a sweeping new privacy law that imposes significant changes to how businesses collect, store, sell, and process consumer "personal information," and will give give California residents broad rights to inquire about what personal information has been collected, with whom it has been shared, and how it may be deleted. The CCPA goes into effect January 1, 2020. Its final status, however, is far from clear.

Below is a history of the CCPA, a summary of its key elements as adopted, including recently adopted technical amendments, and practical takeaways for covered entities as the law moves from passage to 2020 enforcement.

CCPA Background

In the aftermath of the Cambridge Analytica scandal, and in the footsteps of Europe's General Data Protection Regulation ("GDPR"), California privacy advocates introduced a ballot initiative on October 12, 2017 called "The Consumer Right to Privacy Act of 2018" (No. 17-0039). The ballot initiative largely mirrored what is now the language in the CCPA. Due to the challenges of changing laws passed through California's direct ballot initiative, including the requirement that a ballot initiative can only be undone by two-thirds of the popular vote (or else modified by a 70% vote from both state houses), the California legislature agreed to pass the CCPA in exchange for the ballot initiative being withdrawn. Because it was a ballot initiative and would would have been voted on by the California voters during the recent November election cycle, the last day to withdraw the ballot measure was on June 28, 2018. Accordingly, the CCPA was passed unanimously on June 28, 2018 by the California legislature and signed by the governor the same day.

Because the CCPA was passed in one day, it was for the most part poorly written. Accordingly, California lawmakers almost immediately began the amendment process by introducing Senate Bill 1121 (SB-1121) as a cleanup meant to make technical corrections to the law. Those amendments were the subject of a contentious battle between interested stakeholders. On August 6, 2018, a group of business stakeholders, including the California Chamber of Commerce, Association of National Advertisers, California Bankers Association, and Retail Industry Leaders Association, sent a letter to California legislators and encouraged various amendments to fix aspects of the bill that "would be unworkable and that would result in negative consequences unintended by the authors," such as: (1) extending the compliance deadline from January 1, 2020; (2) clarifying the definition of consumer and "personal information" to avoid conflicts of law; (3) clarifying the scope of obligations on businesses relating to the identification and deletion of data; and (4) addressing technical inconsistencies. On August 13, 2018, a coalition of consumer advocacy groups responded by arguing "the sky is not falling, as industry suggests" and claimed the business community's proposed changes would "fundamentally water down" the CCPA's privacy protections. And on August 22, 2018, California AG Xavier Becerra sent a letter to express his concern that the CCPA "imposes several unworkable obligations and serious operational challenges" upon the AG's office, including: (1) requiring the AG to provide opinions to businesses; (2) impose penalties in conflict with the California Constitution; (3) requiring the AG to provide notice prior to enforcement actions; (4) requiring the AG to issue implementing regulations within one year of the law's passage; and (5) by not having a more expansive private right of action.

On September 5, 2018, SB-1121 was finalized on the last day of the legislature's current legislative session, and sent to the governor's desk for signature. It was recently signed into law by the governor. The amendment, which is described in greater detail below, is largely responsive to the AG's complaints, and is seen as the first step in what may be a lengthy fight over what the final law will look like when it takes effect January 1, 2020.

Key Elements Of New Law As Adopted

Who Is Covered?

Businesses

As adopted, the CCPA applies to: (1) any for-profit entity (e.g., sole proprietorship, LLC, corporation); that (2) does business in California; (3) collects or directs to be collected consumer personal information, or determines the purposes and means of processing said personal information; and (4) satisfies any of the following three thresholds:

- Annual gross revenue in excess of $25 million (the CCPA does not specify whether the "gross revenue" is California only, nationwide, or global turnover);
- Annually buys, receives, sells, or shares the "personal information"[1] of 50,000 or more California residents; or
- Derives 50% or more of annual revenues from selling consumer "personal information".

The International Association of Privacy Professionals estimates at least 500,000 U.S. businesses will fall within the scope of the CCPA.

Consumers

The CCPA's definition of "consumer" is equally broad. The CCPA defines "consumer" as a natural person who is a California resident, as defined in 18 CCR § 1704, however identified, including by any unique identifier. This definition therefore not only encompasses a "consumer" in the traditional sense (i.e., someone that has purchased a product from a business), but also any "individual" in California that is a California resident. This ostensibly would include employees of businesses, individuals who enter into commercial transactions with other businesses, and non-consumers of particular business. The business community is already lobbying the California legislature to narrow this definition.

What Is Covered?

The CCPA governs how businesses treat "consumer" "personal information." The CCPA defines "personal information" broadly to include 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 CCPA does not define "household." This definition includes, but is not limited to:

- Identifiers such as 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";
- Any categories of personal information already described under California law;
- Characteristics of protected classifications under California or federal law (e.g., race, religion, sexual orientation, gender identity, gender expression, age, etc.);
- 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, but not limited to, "browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement";
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information;
- Education information (as defined in the Family Education Rights and Privacy Act); and
- "Inferences drawn from any of the information identified" above "to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."

Personal information does not include publicly available information.

SB-1121 limits the definition “personal information” by stating that IP address, geolocation data, and web browsing history would constitute personal information only if the data “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 amendment does not define “household.”

New Consumer Rights

Under the CCPA, as adopted, consumers are given a broad suite of new rights.

- **Right of Disclosure**. Consumers will be permitted to request that a business disclose both the categories and specific pieces of the personal information collected.
- **Right of Deletion**. Consumers will be permitted to request that a business delete personal information it has collected about the consumer, including all data in the possession of the businesses’ vendors. There are several exceptions to this right / obligation, including if the information requested to be deleted is necessary for the business or service provider to maintain the consumer’s personal information 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 the business’s 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;
    - Debug 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 by law;
    - Comply with a legal obligation (the CCPA does not define or limit the phrase “legal obligation”); or
    - To enable solely internal uses of the personal information that are “reasonably aligned” with the expectations of the consumer based on the consumer’s relationship with the business.
- **Right of Portability**. Consumers will be permitted to request that a business provide the consumer with a copy of his or her personal information in a readily usable format that can be transferred to another entity easily; and
- **Right to Opt-Out**. Consumers will be able to request that a business not sell personal data to third parties.

New Business Obligations

In addition to responding to consumer requests for the above information, businesses will have additional obligations under the new law.

- **Duty of Disclosure**. Covered businesses will be required to disclose to a consumer “at or

before the point of collection" the "categories of personal information to be collected and the purposes for which the categories of personal information" will be used. Businesses will be prohibited from collecting additional categories of personal information or use personal information collected for additional purposes without first providing the consumer with notice consistent with this section.

- **Update to Privacy Policy / Notices** . Businesses will be required to establish a "clear and conspicuous" link on their website entitled "Do Not Sell My Personal Information." This page will enable consumers to exercise the right to opt-out of the sale of their personal information. If the consumer opts-out, the business must wait at least 12 months from the date the consumer opts-out before requesting the consumer authorize the sale of his or her personal data. A business that collects personal information about consumers must also disclose the consumer's rights to request the deletion of the consumer's personal information. That disclosure must include two or more designated methods for submitting requests for deletion, including at a minimum a toll-free telephone number, and if the business maintains a website, the website address.
- **Anti-Discrimination Provisions**. Businesses will be prohibited from discriminating against any consumer for exercising their rights under the new law. This means, in practical terms, denying a consumer goods or services, charging different prices, or providing a lower quality of services or goods. Businesses will, however, be able to charge a different price or level of good or service if the difference is "reasonably related to the value" of the consumer's data. The new law also allows businesses to offer consumers "financial incentives" for the collection and sale of their personal information.

Exemptions

The CCPA, as adopted, contains important exemptions for businesses already collecting "personal information" (as that phrase is defined under the CCPA) under the Confidentiality of Medical Information Act ("CMIA"), Health Insurance Portability and Availability Act of 1996 ("HIPAA"), Fair Credit Reporting Act ("FCRA"), Gramm-Leach-Bliley Act ("GLBA"), and Driver's Privacy Protection Act of 1994 ("DPPA").

Covered entities should note, however, that these exemptions may only be partial. The definition of "personal information" under the CCPA is, in most cases, broader than the definition of covered information in the statutes listed above. Thus, it is plausible that a business could be collecting the broad array of "personal information" under the CCPA, but only a small subset of that information is covered under the statutes listed above.

Below is a summary of each exemption, as adopted and amended:

- **Health Information Exemption:** The CCPA, as adopted, exempts "protected or health information" collected by a covered entity pursuant to the CMIA or governed by the privacy, security, and breach notification rules issued by the Department of Health and Human Services (45 CFR Parts 160 and 164), established pursuant to HIPAA. SB-1211 cleaned up this exemption up by clarifying the types of information covered: (1) "medical

information"[2] governed by the CMIA; (2) "protected health information" [3] "collected by a covered entity or business associate" governed by the privacy, security, and breach notification rules set forth under HIPAA and its implementing regulations; (3) a "provider of health care" governed by the CMIA or a covered entity under HIPAA, "to the extent the provider or covered entity maintains patient information in the same manner" as medical information or protected health information as described above; and (3) information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

- **Consumer Reporting Exemption**: The CCPA, as adopted, does not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by 15 U.S.C. § 1681a, and as that information is used pursuant to the Fair Credit Reporting Act (15 U.S.C. §§ 1681, *et seq*.).
- **GLBA Exemption**: The CCPA, as adopted, does not apply to "personal information" that is "collected, processed, sold, or disclosed" pursuant to the federal GLBA and its implementing regulations[4] if "if it is in conflict with that law." SB-1121 amended this exemption by removing the "in conflict" provision, but making clear that a business so exempted will still be subject to the data security / breach requirements under the CCPA. SB-1121 also added an exemption for "personal information" collected under the California Financial Information Privacy Act ("CFIPA").[5]
- **Driver's Protection Act Exemptions**: The CCPA, as adopted, does not apply to personal information collected, processed, sold, or disclosed pursuant to the DPPA[6] "if it is in conflict with that act." SB-1121 removes the "in conflict" language, but states that exempt businesses will nonetheless be subject to the data security / breach requirements under the CCPA.

Enforcement

- **AG Opinions / Guidance**. The CCPA allows any "business or third party" to seek the opinion of the California AG for "guidance on how to comply" with the CCPA.
- **AG Implementing Regulations**. The AG has one year from the effective date of the CCPA to implement enforcing regulations.
- **Private Right of Action**. The CCPA allows for a private right of action only if the consumer's personal information is unencrypted, non-redacted, and has been the subject of an unauthorized "access and exfiltration, theft or disclosure as a result of the businesses' violation of the duty to implement and maintain reasonable security procedures and practices…to protect the personal information." A consumer bringing such action may seek the greater of actual damages or statutory damages (capped at $750 per consumer, per incident), in addition to injunctive and declaratory relief if appropriate.
- **Safe Harbor**. Prior to filing a private right of action, a consumer must provide a business with written notice of any intent to sue at least 30 days in advance of bringing any such

suit. The consumer must also notify the California Attorney General within 30 days of filing the suit. The Attorney General must notify the consumer within 30 days after receiving such notice if the Attorney General's office intends to prosecute. Business have 30 days from notice of alleged noncompliance to cure any alleged violation.
- **Civil Penalties**. The CCPA allows for the collection of civil penalties by the Attorney General up to $7,500 per violation to be assessed pursuant to California's Unfair Competition Law ("UCL") at California Business and Professions Code § 17206.

New Amendments

California AG Objections

On August 22, 2018, California AG Xavier Becerra sent a letter to California lawmakers to express his concern that the CCPA "imposes several unworkable obligations and serious operational challenges" upon the AG's office. The AG has five primary concerns with the existing language of the CCPA:

- **AG Advice and Safe Harbor**. The CCPA requires the AG to provide opinions to "[a]ny business or third party" as well as warnings and an opportunity to cure before the business can be held accountable for a violation of the CCPA. AG Becerra says requiring the AG's office to provide "legal counsel at taxpayers' expense to all inquiring businesses creates the unprecedented obligation of using public funds to provide unlimited legal advice to private parties." AG Becerra also claims this provision creates a potential conflict of interest by having the AG's office provide legal advice to parties who may be violating the privacy rights of Californians – "the very people that the AGO is sworn to protect." AG Becerra queries – "[w]hat could be more unfair and unconscionable than to advantage violators of consumers' privacy by providing them with legal counsel at taxpayer expense but leaving the victims of the privacy violation on their own?"
- **Unconstitutionality of Penalties**. The AG claims the CCPA's civil penalty provisions are "likely unconstitutional" because the penalties would be applied under California's Business and Professions Code § 17206. Because Business and Professions Code § 17206 was enacted by the voters through Proposition 64 in 2004, and cannot be amended through legislation pursuant to the California Constitution (Article II, § 10), the current penalty provision may be void. AG Becerra proposes to "address this constitutional infirmity by simply replacing the CCPA's current penalty provision with a conventional stand-alone enforcement provision that does not purport to modify the UCL."
- **AG Notice**. AG Becerra claims the requirement that private litigants give notice to the AG before filing suit is "unnecessary" and "has no purpose as the courts not the Attorney General decide the merits of private lawsuits." AG Becerra claims this provision "imposes unnecessary personnel and administrative costs on the AGO and it, too, should be eliminated."
- **Lack of Resources**. The CCPA requires the AG's office to conduct rulemaking within one year, but the AG argues there are insufficient resources for the AG's office to carry out

the rule-making or carry out implementation thereafter. “The nature and pace of the rule-making process,” writes Becerra, “especially in light of the broad public interest in privacy issues, does not lend itself to a short-circuited timeframe to formulate the rules that will govern the oversight and enforcement of the CCPA’s privacy rights.” AG Becerra notes that a one-year deadline to establish implementing regulations for the CCPA are unattainable, and the AG’s office must be given a sufficient and realistic amount of time to issue “strong, enforceable regulations.”
- **Private Right of Action**. The AG believes there should be a private right of action to sue under the CCPA because a lack of a private right of action will substantially increase the AG’s office’s need for new enforcement resources.

SB-1121 Amendment

In addition to clarifying the definition of “personal information” and the relevant exemptions (highlighted above), the amendments in SB-1121 also extend the AG’s one-year deadline to issue implementing regulations by six months, from January 1 to July 1, 2020 and clarify the civil penalties are limited to $2,500 for each violation, and up to $7,500 for each intentional violation (and are removed from Business and Professions Code § 17206).

Key Takeaways

The Law Will Likely Change Before January 1, 2020

Although the CCPA does not take effect until January 1, 2020, it will likely change between now and then. As can be seen in SB-1121, amendments are only just beginning to trickle in. The law will likely be revised several times before its effective date. Thus, although compliance efforts now will mitigate costs in the future, the particular nuances of the law have yet to be finalized.

If Unchanged, The New Law Will Change The Way You Use Cookies

The CCPA requires businesses to disclose to consumers “at or before the point of collection” the “categories of personal information to be collected and the purposes for which the categories of personal information shall be used.” Because the phrase “personal information” is defined broadly to include IP addresses, “Internet or other electronic network activity information” such as “browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement”, this means businesses will need to disclose to consumers at the point of placement of a cookie the nature of the information collected by the cookie, and the purposes for which the personal information will be used once collected. Unless changed, this will require a change in how businesses who are not otherwise covered under the GDPR handle cookie disclosures. For example, if your business places 45 cookies for each web experience, you will be required to disclose the categories of personal information collected through those cookies (e.g., IP address, browsing history, etc.) and explain why you collect such information (e.g., statistical, marketing, user experience purposes).

Data Segregation And Cybersecurity Are Key

If the current definition of "personal information" remains, businesses should work to have a robust understanding of their current data flows, map all data received and transmitted (including to and from vendors), and think through appropriate ways to segregate the data. Undertaking this process now will help mitigate the compliance burden come 2020 as it will make it easier for you and your business to respond to consumer demands for disclosure, deletion, and portability. Sounds cybersecurity practices are also key to mitigating liability under the new law. A private right of action, for example, may only be brought if the personal information of a consumer is both unencrypted and unredacted. Thus, if a business encrypts the personal information of the consumer, and that information is stolen, there will be no private right of action under the CCPA. That does not mean, however, that the business would be completely off the hook. The California data breach notification law would still require a business to notify consumers (and potentially the Attorney General) if the encrypted information was accessed or taken along with the encryption key. No such language is present in the CCPA. The new law also only permits a private right of action if the business violates its duty to "implement and maintain reasonable security procedures and practices…to protect the personal information." This means that businesses should audit their current cybersecurity practices, policies, and procedures to ensure they are matching industry standards and building a robust cyber resilient framework to serve as a defense to any future causes of action under this new law.

If you or your company would like more information about the CCPA and how it may impact your operations, the Dentons Privacy and Cybersecurity team is ready to help. From data mapping to cybersecurity risk assessments, our team is well suited to prepare your business for compliance in a way that remains flexible to the extent the law changes further prior to its January 1, 2020 implementation date.

[1] The CCPA defines "personal information" to include IP addresses. The CCPA therefore applies, ostensibly, to any business that receives 50,000 IP addresses per year on its website, which is only an average of approximately 137 unique visitors per day.

[2] The phrase "medical information" under the CCPA is defined by California Civil Code § 56.05(j), which defines the phrase to mean "any individually identifiable information" in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." Cal. Civ. Code § 56.05(j). "Individually identifiable" under Civil Code § 56.05(j) means that the medical information "includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." *Id*.

[3] The phrase “protected health information” under the CCPA is defined by 45 C.F.R. § 160.103 to mean “individually identifiable health information” that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. Individually identifiable health information is defined as “information that is a subset of health information, including demographic information collected from an individual” and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (3) that identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual. The definition of “protected health information” excludes individually identifiable health information: (i) in education records covered by the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); (ii) records described at 20 U.S.C. § 1232g(a)(4)(B)(iv); (iii) employment records held by a covered entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years. 45 C.F.R. § 160.10(1)-(2).

[4] The GLBA places restrictions on how covered entities collect, use, and disclose certain “nonpublic personal information” relating to consumers. “Nonpublic personal information” is defined under the GLBA as “personally identifiable financial information – (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution. 18 U.S.C. § 6809(4)(A). Such information includes any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information. 18 U.S.C. § 6809(4)(B). The GLBA’ implementing regulations, promulgated and enforced by the Federal Trade Commission (“FTC”). The FTC adopts the same definition of nonpublic personal information, and defines “personally identifiable financial information” to mean any information: (i) a consumer provides to obtain a financial product or service from the covered entity; (ii) about a consumer resulting from any transaction involving a financial product or service between the covered entity and the consumer; or (iii) the covered entity otherwise obtains about a consumer in connection with providing a financial product or service to the consumer. 16 CFR § 313.3(o)(1)(i)-(iii). Examples of personally identifying financial information include: (A) information a consumer provides to the covered entity on an application to obtain a loan, credit card, or other financial product or service; (B) account balance information, payment history, overdraft history, and credit or debit card purchase information; (C) the fact that an individual is or has been one of the covered entity’s customers or has obtained a financial product or service from the covered entity; (D) any information about the consumer if it is disclosed in a manner that indicates the individual is or has been a consumer; (E) any information that a consumer provides to the covered entity or that the covered entity or its agent otherwise obtain in connection with collecting on, or servicing, a credit account; (F) any information the covered entity collects through an Internet “cookie” (an information collecting device from a web server); and (G) information from a consumer report. Information not included as personally identifiable financial information includes information that does not

identify a consumer, “such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.” 16 C.F.R. § 313.3(o)(2)(i)-(ii).

[5] The California Financial Information Privacy Act provides for greater privacy protections than those provided in the GLBA, and likewise regulates the collection, usage, and storage of “nonpublic personal information.” Cal. Fin. Code § 4051. The CFIPA defines “nonpublic personal information” the same as the GLBA, and the phrase “personally identifiable financial information” the same as the GLBA and its implementing regulations. Cal. Fin. Code §§ 4052(a)-(b).

[6] “Personal information” is defined under the DPPA means “information that identifies an individual, including an individual’s photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver’s status.