AN INFORMATIONAL HEARING OF THE ASSEMBLY COMMITTEE ON PRIVACY & CONSUMER PROTECTION

Understanding the Rights, Protections, and Obligations Established by the California Consumer Privacy Act of 2018: Where should California go from here?

February 20, 2019
9:00 a.m.
State Capitol, Room 4202

Article I, Section 1 of the California Constitution: *All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.*

Section 1 of the California Consumer Privacy Act of 2018 (AB 375, Chapter 55, Statutes of 2018): *In 1972, California voters amended the California Constitution to include the right of privacy among the "inalienable" rights of all people. The amendment established a legal and enforceable right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information.*

I. Background

California's constitution provides that, among other rights, all people have an inalienable right to pursue and obtain privacy. This, effectively, protects an individual's fundamental right to privacy from both governmental and private actors.

At the same time, however, this state has grappled for many years with the issue of protecting one's privacy, and private information, in an increasingly digital and data-driven world. In the years since the passage of the 1972 constitutional amendment recognizing the right of privacy, the Legislature has adopted specific mechanisms to safeguard Californians' privacy. These laws include the Privacy Rights for California Minors in the Digital World Act (2013); California Online Privacy Protection Act (2003); and Shine the Light (2003), a California law intended to give Californians the "who, what, where, and when" of how businesses handle consumers' personal information.

Most recently, last year, California passed a landmark piece of privacy legislation, AB 375 (Chapter 55, Statutes of 2018), which enacted the "California Consumer Privacy Act of 2018" (CCPA). Since its passage, this Committee has received many requests for clarification on the rights, protections, and obligations established by the CCPA. Numerous stakeholders have urged additional refinement of the law – ranging from suggestions on how to further clarify and

address perceived workability issues from a business standpoint, to suggestions on how to strengthen the law from a consumer and privacy protections standpoint.

Thus, on February 20, 2019, the Assembly Privacy & Consumer Protection Committee will hold an informational hearing to hear from various stakeholders on the CCPA. The Committee seeks to bring greater understanding to these new rights and protections (and, inversely, business obligations), and to also explore how the Legislature might further refine the CCPA in a manner that will ensure the new law operates in the privacy protective manner originally envisioned, while simultaneously resolving workability issues or confusion for business communities.

In doing so, the Committee will explore, among other things, the following:

- What are the rights and protections of Californians under the CCPA?
- What are the obligations of businesses under the CCPA?
- How do these rights and obligations compare to and align with the European Union's General Data Protection Regulation (GDPR)?
- How are companies moving toward compliance?
- What process has the Department of Justice (DOJ) set for the regulations and what progress has the DOJ made in those regulatory efforts?
- What are the next steps of the DOJ?
- What are the workability and clarity issues that stakeholders see as requiring legislative solutions in 2019?
- Are there steps that California should take to maintain its lead in privacy in the nation?
- What federal preemption efforts are present at the national level?
- How can the Legislature ensure that privacy protections are both consumer friendly and workable for business, in order for the CCPA to have the utmost utility?

II. CCPA Background

On June 28, 2018, the California Legislature unanimously passed, and the Governor signed AB 375, a significant expansion of data privacy protections for Californians. That new law, the CCPA, guarantees consumers certain rights and protections with respect to the collection and sale[1] of their personal information (PI). These rights and protections include the following:

[1] Notably, "sale" under the CCPA generally includes selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration. (*See* Civ. Code Sec. 1798.140.) "Collecting" includes buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior. (*Id.*)

- **Right to Access PI** – Grants consumers the right to request the categories and specific pieces of PI that a business collects about them, and requires businesses to provide that information only upon receipt of a verifiable consumer request, as specified. Requires businesses to inform consumers of the categories of PI to be collected and the purposes for which the categories of PI will be used, and restricts the collection of additional categories without providing the consumer notice. Specifies that these rights, however, do not require a business to retain any PI collected for a single, one-time transaction, if such information is not sold or retained by the business or to re-identify or otherwise link information that is not maintained in a manner that would be considered PI. (Civ. Code Sec. 1798.100.)
- **Right to Know What PI is Being Collected** – Generally grants consumers the right to request, and requires a business that collects PI about the consumer to disclose, upon receipt of a verifiable consumer request from the consumer: (1) the categories of PI it has collected about that consumer; (2) the sources from which the PI is collected; (3) the business or commercial purpose for collecting or selling PI; (4) the categories of third parties with whom the business shares PI; and (5) the specific pieces of PI it has collected about that consumer. (Civ. Code Sec. 1798.110.)
- **Right to Know Whether Personal Information is Sold or Disclosed** – Grants consumers the right to request, and requires any business that sells or discloses the PI of the consumer for a business purposes to disclose, upon receipt of a verifiable consumer request from the consumer, the categories of PI the business: (1) collects about the consumer; (2) disclosed for business purposes; and (3) sold about the consumer and the categories of third parties to whom the business sold the PI. Prohibits a third party from selling PI about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out under the bill. (Civ. Code Sec. 1798.115.)
- **Right to Deletion of PI** – generally provides consumers the right to request that a business delete any PI collected *from* the consumer (as opposed to "about" the consumer) from its records and requires businesses to direct services providers to do the same, subject to various exemptions. (Civ. Code Sec. 1798.105.)
- **Right to Say "No" to the Sale of PI** – provides consumers, 16 years of age and over, the "right to opt-out" of the sale of their PI to third parties. Prohibits businesses from selling the PI of consumers under the age of 16, unless the consumer or his or her parent/guardian affirmatively authorizes the sale of the minor's information, as specified. Specifically, minors who are at least 13 years of age and less than 16 years of age personally have the "right to opt-in" to the sale of their PI. For minors under the age of 13, the minor's parent or guardian would be required to opt-in on the minor's behalf. (Civ. Code Sec. 1798.120.)
- **Right to Equal Service and Price –** Prohibits businesses from discriminating against any consumer for exercising any of the rights listed above. Expressly prohibits discrimination by

any of the following: (1) denying goods or services to the consumer; (2) charging different prices, such as through the use of discounts or other benefits, or imposition of penalties; (3) providing a different level of quality of goods or services; or (4) suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. However, a business may still offer certain financial incentives, as long as they are not unjust, unreasonable, coercive, or usurious. Specifically authorizes businesses to offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided by the consumer's data, as specified. (Civ. Code Sec. 1798.125.)

All of these rights are subject to various express exemptions. For example, the CCPA specifies that the obligations imposed on businesses by this title shall not restrict a business's ability to:

- Comply with federal, state, or local laws.
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
- Exercise or defend legal claims.
- Collect, use, retain, sell, or disclose consumer information that is de-identified or in the aggregate.
- Collect or sell a consumer's PI if every aspect of that commercial conduct takes place wholly outside of California, as specified.

The bill also provides various exemptions for certain types of information, such as medical information governed under state and federal privacy laws, as specified; and PI collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act or the California Financial Information Privacy Act. (*See* Civ. Code Sec. 1798.145 for these and other exemptions.)

The rights and protections established by the CCPA are largely enforceable by way of public enforcement, except in situations involving a data breach. In the case of data breach, the new law allows for a private right of action, after notice and a 30-day right to cure (in the event a right to cure is possible), as specified. Where a civil action is initiated pursuant to this private right of action, the consumer may seek damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages.

Aside from this limited basis for initiating a private right of action, the CCPA provides for exclusive enforcement of violations by the Attorney General (AG). Specifically, a business shall be in violation of the CCPA if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any person, business, or service provider that violates the CCPA is subject to an injunction and civil penalties of up not more than $2,500 for each violation or $7,500 for each intentional violation, consistent with California's Unfair

Competition Law (Civ. Code Sec. 17206). The CCPA also specifies that any civil penalty assessed, and the proceeds of any settlement of an action brought by the AG are to be deposited in the Consumer Privacy Fund in the General Fund, with the intent to fully offset any costs incurred by the state courts and the AG in connection with the CCPA.

The CCPA also authorizes a business or third party to seek guidance from the AG on how to comply with the provisions of the law.

III. SB 1121 (Chapter 735, Statutes of 2018)

Enacted by AB 375, the CCPA represents a legislative effort to reach an agreement on issues relating to the collection and sale of consumers' PI by businesses, both online and otherwise. Those same issues were also the subject of initiative measure, which would have been placed on the November 2018 ballot for Californian voters' consideration in the absence of a legislative solution by June 28, 2018—the deadline to remove an initiative from the November ballot. Given the abbreviated deadline to adopt the CCPA in time for the proponents to remove their proposal from consideration, numerous drafting errors were contained in the legislation as initially adopted. Many of those errors were addressed in a preliminary clean-up bill at the end of the 2017-2018 legislative session, in SB 1121, as were several policy suggestions made by the AG. That bill was signed by Governor Brown on September 23, 2018.

As part of those first technical and clarifying changes made to the CCPA, SB 1121:

- Ensured that the private right of action applies only to the CCPA's section on data breach and not to any other section of that law, as specified.
- Added a clarifying exemption to for newsgathering activities, as specified.
- Clarified and revised the existing CCPA exemptions relating to Health Insurance Portability and Accountability and Confidentiality of Medical Information Act.
- Clarified and revised the existing CCPA exemptions for PI collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act or the Drivers Privacy Protection Act.
- Created an exception to the delayed implementation date of the CCPA to ensure the CCPA provision providing for preemption of local rules, regulations, codes, ordinances, and other laws would take effect immediately.
- Provided a technical amendment to the definition of "PI" to clarify that the enumerated items under that definition are "PI" if the enumerated item identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.
- Made other technical and clarifying changes, including, among other things, replacing the term "verified request" with "verified consumer request" throughout the CCPA to accurately reflect the definitions contained therein.

Furthermore, with respect to CCPA's provisions relating to the AG, specifically, SB 1121:

- Removed any reference to the Unfair Competition Law (Bus. & Prof. Code Sec. 17206, specifically) to avoid constitutionality issues and, instead, established a standalone enforcement statute for the AG whereby any business, service provider, or other person that violates the CCPA shall be subject to an injunction and liable for a civil penalty of not more than $2,500 for each violation and $7,500 for each intentional violation, as specified.
- Eliminated the "80/20" percentage split in how civil penalties are allocated in the Consumer Privacy Fund – *all* penalties, instead, will be deposited into the Fund with the intent to fully offset any CCPA-related costs incurred by the courts and the AG.
- Extended the deadline for the AG to solicit public participation and adopt regulations, as otherwise specified, from January 1, 2020 to July 1, 2020. Relatedly, added that the AG shall not bring an enforcement action until six months after the publication of the final regulations issued pursuant to this provision, or July 1, 2020, whichever is sooner.
- Removed a requirement that the AG establish specific regulations within one year of passage of AB 375 (*i.e.*, by June 28, 2019) from one of four CCPA provisions that contain this earlier timeframe for specific regulations.
- Removed the "gatekeeping" function of the AG from the section establishing a private right of action, as specified (wherein the AG could have otherwise precluded a consumer from bringing a lawsuit against a business, among other things).

IV. The European Union's General Data Protection Regulation

California, while the first in the nation, was not the first legislative body to promulgate expansive rules and legislation on the issue of how consumers' personal data is collected, sold, and protected from privacy and data breaches in a data-driven world. The European Union passed the General Data Protection Regulation (GDPR) on April 14, 2016, effective May 25, 2018, on many of these same issues. With the GDPR in mind at the time of its drafting, the CCPA sought to include similar privacy protections for consumers. Significantly, both laws are technology-neutral to ensure their longevity and the CCPA shares many similarities to the GDPR (in some ways, more so than the privacy initiative which would have been on California's November 2018 ballot), as outlined on the following chart:

Protections	EU Privacy Law (GDPR)	Privacy Initiative	CA Consumer Privacy Act (CCPA)
Do businesses provide notice about information practices?	✓	✓	✓
Do you have the right to know information a business has about you?	✓	✓	✓
Can you prohibit a business from selling your information?	✓ *Opt-in	✓ *Opt-out	✓ *Opt-out
Can you ask a business to give you the specific information they have about you? (portability)	✓	⊘	✓
Can you ask a business to delete the information they have about you?	✓	⊘	✓ * Only information the business has collected *from* the consumer
Are businesses required to safeguard your data?	✓	✓	✓
Can you enforce your rights through a lawsuit?	✓	✓	✓ *Data breach only
Do minors get special protections?	✓	⊘ *parents exercise rights under 18	✓ *minors who are 13 and up to 16 years of age have opt-in rights

V. Attorney General regulatory requirements

In addition to its enforcement responsibilities, and the recognition of the AG's ability to provide guidance, the CCPA requires that the AG solicit broad public participation and adopt regulations for purposes of the CCPA on or before July 1, 2020. As noted in Section III, above, the AG cannot bring an enforcement action until six months after publication of the final regulation, or July 1, 2020 – whichever date comes first. The CCPA expressly includes several areas for AG regulations, which can be generally described as:

- Updates to categories of personal information.
- Updates to the definition of unique identifiers.
- Establishing any exceptions necessary to the CCPA to enable businesses to comply with other state and federal laws, including, but not limited to, those relating to trade secrets and intellectual property rights.
- Establishing rules for the submission and handling consumer opt-out requests and for the development of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of their opportunity to opt-out.

- Adjusting the monetary threshold for purposes of the "business" definition.
- Establishing rules, procedures, and necessary exceptions to ensure that the notices and information that businesses are responsible for are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings.
- Establishing rules and procedures to further the purposes of the CCPA's sections on the consumers' rights to know what categories and specific pieces of information has been collected/sold about them, as specified. This includes, among other things, rules and procedures governing a business's determination that a request for information received by a consumer is a "verifiable consumer request." (*See* Civ. Code Sec. 1798.185.)

In line with these requirements, the AG previously announced that it would be holding numerous statewide forums to collect feedback from stakeholders early in the rulemaking process. As part of this announcement, the DOJ invited all interested persons and parties to submit comments regarding the CCPA regulations at any of the six statewide forums, via mail or email.

VI. Post-CCPA: Other State Laws and Federal Efforts

Since the passage of the CCPA, numerous other states have introduced similar laws that appear to be modeled, at least in part, on the CCPA. Such states reportedly include, among others: Hawaii (SB 418), Massachusetts (SD 341), Mississippi (HB 2153), New Mexico (SB 176), New York (S00224), North Dakota (HB 1485), Rhode Island (S0234).[2]

That being said, on the federal level, several bills have also been introduced to address this issue of data privacy, which, if successful, could either expressly or implicitly preempt these efforts, as well as the CCPA—thus eroding the rights and protections established for Californians as of last year. Among these is Senator Marco Rubio's American Data Dissemination Act, which would expressly preempt state privacy laws, such as the CCPA and require instead that the Federal Trade Commission submit recommendations for privacy rules for review by Congress. Senators Amy Klobuchar and John Kennedy have also introduced the bipartisan Social Media Privacy and Consumer Rights Act of 2019, which would enable consumers to opt-out of the collection and use of their personal data, and would contain data breach notification requirements, among other things.

[2] (*See* Privacy & Security Law Blog, *"Copycat CCPA" bills introduced in states across the country* (Feb. 8, 2019) <https://www.privsecblog.com/2019/02/articles/california-consumer-protection-act-ccpa/copycat-ccpa-bills-introduced-in-states-across-country/> [as of Feb. 16, 2019].)