Expert Q&A: The California Consumer Privacy Act of 2018 (CCPA)

PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

An Expert Q&A with Morrison & Foerster's Purvi G. Patel, Nathan D. Taylor, and Alexandra E. Laks, examining California's surprise passage of the landmark California Consumer Privacy Act of 2018 (CCPA) on June 28, 2018, and its September 23, 2018 amendments.

California became the first state to enact comprehensive data protection legislation with its June 28, 2018 passage of the California Consumer Privacy Act of 2018 (CCPA) (2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (WEST)). The expansive new privacy law, which passed within a week of its introduction and was amended on September 23, 2018, imposes significant obligations and restrictions on businesses across the US that handle the personal information of California residents.

Practical Law asked Purvi G. Patel, a leading consumer privacy litigation partner from Morrison & Foerster's Los Angeles office, along with her colleagues in the Privacy & Data Security practice group, Washington DC-based partner Nathan D. Taylor and San Francisco-based associate, Alexandra E. Laks, to discuss the recently amended CCPA's requirements and how business should start preparing to comply with the new law in advance of its January 1, 2020 operative date.

WHAT IS THE CCPA?

The CCPA is arguably the most expansive consumer privacy legislation in US history. The California legislature rapidly passed the statute on June 28, 2018 to avoid the introduction of a similar controversial privacy ballot initiative with the same name.

The legislature revisited the Act just two months later to address drafting errors and make minor amendments and clarifications, passing Senate Bill 1121 (CCPA Amendments) on August 31, 2018, before adjourning for the year (2018 Cal. Legis. Serv. Ch. 735 (S.B. 1121) (WEST)). Governor Jerry Brown signed the CCPA Amendments into law on September 23, 2018.

WHO DOES THE CCPA PROTECT?

The CCPA protects "consumers," which it defines as California residents. This means that the CCPA governs how a business handles personal information relating to any California resident, regardless of a business's relationship with the individual.

WHO MUST COMPLY WITH THE CCPA'S REQUIREMENTS?

An entity must comply with the CCPA if it:

- Collects a consumers' personal information.
- Determines the purposes and means of processing that personal information.
- Does business in California, and meets one of the following thresholds:
  - has annual gross revenues in excess of $25 million;
  - annually buys, receives for its commercial purposes, sells, or shares for commercial purposes personal information relating to 50,000 or more consumers, households, or devices; or
  - derives 50% or more of its annual revenue from selling consumers' personal information.

An entity must also comply if it controls or is controlled by a business that meets the above requirements and shares common branding with the entity, such as a shared name, service mark, or trademark.

WHAT QUALIFIES AS PERSONAL INFORMATION UNDER THE STATUTE?

The CCPA defines personal information broadly to include any information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked to, directly or indirectly, a particular consumer or household. Personal information specifically includes items that indirectly identify a unique person, such as an alias, unique personal identifier, or other online identifier.

Personal information also includes, but is not limited to, 11 enumerated categories of information relating to consumers. Several of those categories involve information that US privacy laws do not typically include as personal information, such as:

- Commercial information, including a consumer's purchasing or consuming histories or tendencies.
- Internet activity, such as a consumer's browsing patterns, search history, or interaction with a website, application, or advertisement.
- Inferences drawn about the consumer from any of the enumerated categories of personal information to create a profile about the consumer reflecting, for example, the consumer's preferences or characteristics.

Additionally, while the CCPA defines personal information in detail, the Act's reference to information linked with a particular "household" is undefined, and could include any child, spouse, or even roommate, creating uncertainty regarding its scope.

WHAT CONSUMER RIGHTS AND COMPLIANCE REQUIREMENTS ARE OUTLINED IN THE CCPA?

The CCPA provides consumers with the right to request deletion of personal information, access personal information, opt out of the sale of personal information, and be free from discrimination. The Act imposes corresponding obligations on businesses to facilitate these rights, including, for example:

- **Deletion.** A business must delete, and direct service providers to delete, any personal information collected about a consumer on request. The CCPA includes nine exceptions to this requirement, which businesses and their counsel must carefully consider when implementing procedures to comply with a consumer's deletion request.
- **Access and portability.** In response to a consumer's request, a business must disclose:
  - the categories of personal information about the consumer that the business collected;
  - the categories of sources from which the personal information was collected;
  - the categories of personal information about the consumer that the business sold to a third party;
  - the categories of personal information about the consumer that the business disclosed for a business purpose;
  - the categories of third parties to whom the business sold or disclosed personal information;
  - the business or commercial purpose for which personal information was collected or sold; and
  - the "specific pieces" of personal information a business collected about an individual.
- The business must provide these disclosures as they relate to the consumer's personal information that the business handled within the year preceding the request and "in a readily useable format that allows the consumer to transmit [the] information from one entity to another entity without hindrance." (2018 Cal. Legis. Serv. Ch. 55, at proposed § 1798.100(d).)
- **Opt out.** In general, businesses must enable and honor consumer requests to opt out of the sale of personal information. For consumers ages 16 and under, however, a business must obtain express consent to sell personal information. To help consumers easily exercise their opt-out rights, a business must include a "Do Not Sell My Personal Information" link in a "clear and conspicuous" location on its website's homepage.
- **Be free from discrimination.** Businesses may not charge different prices or rates to consumers, provide different services, or deny goods or services to consumers who exercise their rights under the CCPA. In some instances, businesses may offer consumers financial incentives to collect, sell, or not delete personal information.

Businesses must disclose these rights to consumers in their online privacy policies and in any California-specific description of consumers' privacy rights. Businesses must also list in their privacy policies the categories of personal information they collected, sold, or disclosed for a business purpose within the last 12 months.

IN PRACTICE, WILL THE CCPA APPLY EVERYWHERE IN THE US? OR, WILL COMPANIES INTERACTING WITH CALIFORNIA RESIDENTS OFFER TWO PRIVACY POLICIES OR ADOPT TWO WAYS OF HANDLING PERSONAL INFORMATION?

Each covered entity must decide whether to extend the CCPA's privacy rights to individuals residing in states other than California. Before making this decision, a business must think through several practical and competitive considerations, including:

- Whether the business can easily and effectively distinguish between information relating to California residents and information relating to residents of other states.
- The customer relations impact of telling non-California customers or employees that they do not have the same privacy rights as individuals in California.
- The legal risks associated with voluntarily making privacy-related representations to consumers across the US and functionally creating a legal obligation in all 50 states to live up to those representations.
- The likelihood that other states may follow California's lead and impose their own privacy obligations, which may or may not track the CCPA.

THE CCPA REQUIRES THE CALIFORNIA ATTORNEY GENERAL (AG) TO SOLICIT BROAD PUBLIC PARTICIPATION TO ADOPT RELEVANT REGULATIONS. WHAT TYPES OF REGULATIONS ARE LIKELY ON THE HORIZON, AND WHAT TYPES OF BUSINESSES SHOULD OFFER COMMENTS OR PARTICIPATE?

Under the CCPA, the AG may adopt implementing regulations to further the Act's purposes as needed. Additionally, the AG is specifically directed to issue regulations, for example, that:

- Clarify the exact information businesses must include in their notices to consumers.
- Define what constitutes a "California-specific description of consumers' privacy rights."
- Prescribe a standardized "Do Not Sell My Personal Information" logo.

- Set forth other processes regarding how businesses must respond to consumer deletion, access, and opt-out requests.
- Add categories of personal information and unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns.

The CCPA Amendments extend the AG's deadline to adopt implementing regulations to July 1, 2020, though there are several rulewriting provisions in the Act that require the AG to issue rules within one year of its passage (that is, June 28, 2019). Because the statute applies broadly across industries, it will be important for businesses across industries to participate in the rulemaking process.

WHAT STEPS SHOULD BUSINESSES SEEKING TO COMPLY WITH THE CCPA TAKE NEXT?

Businesses should start preparations now to meet the CCPA's January 1, 2020 operative date. Although the CCPA Amendments extend the deadline for the AG to issue implementing regulations, and the California legislature may consider additional amendments to the CCPA's provisions, businesses should not wait to take action. For many businesses, adjusting business processes and activities to comply with the CCPA's provisions and putting in place capabilities to honor consumer requests will likely take longer than anticipated.

Immediate steps that businesses should consider, both for compliance purposes and to determine key areas for 2019 advocacy efforts, include:

- **Tracking data streams.** To respond to consumer requests and properly update privacy policies, a businesses must confirm how it handles personal information relating to California residents, including:
  - when and how the business collects the personal information;
  - where, for how long, and on what systems the business stores the personal information; and
  - with whom the business shares the personal information.
- Because the CCPA defines personal information broadly and covers any California resident, it is important to develop an understanding of how the business handles consumers' personal information across the organization (for example, human resources, customer service, or vendor management).
- **Identifying operational challenges that compliance may pose.** A business should consider both:
  - the systems and manual or automated processes it must have in place to implement the CCPA's deletion, access, portability, and opt-out requirements; and
  - which aspects of these requirements are the most burdensome.
- **Developing processes to enable compliance.** A business should develop processes needed to comply with the CCPA's key provisions, including:
  - setting up a toll-free number and web address for consumers to submit requests;
  - designating an individual or team to monitor and respond to consumer requests within 45 days;
  - verifying the identity and authorization of consumers making access or deletion requests;
  - designating mechanisms that enable the business to honor opt-out requests; and
  - updating privacy-related disclosures, such as online privacy policies.
- **Considering alternative business practices.** A business should consider whether and how to change its current practices for handling consumers' personal information, given the CCPA's requirements. For example, in light of the CCPA's broad definition of "sale," which includes disclosures of personal information for valuable consideration, a business could consider its disclosure practices and whether any changes would eliminate the need to provide an opt out.

WHAT IS THE SCOPE OF THE CCPA'S CONSUMER PRIVATE RIGHT OF ACTION?

When the CCPA originally passed, the scope of the consumer private right of action was unclear due to several ambiguities in the provision's text, including whether consumers could sue only for specified data security events or for any violation of the CCPA's obligations. The original CCPA text also required consumers to provide businesses with 30 days to cure alleged violations and notify the AG after filing suit.

In arguably the most critical substantive clarification, the CCPA Amendments confirm that a consumer's right to sue is limited to certain data security incidents involving a business's failure to comply with the duty to maintain reasonable security procedures and adopt practices to protect personal information (as defined under the California safeguards law, Cal. Civ. Code § 1798.81.5(d)(1)(A), which is part of the California Data Protection Act). The CCPA Amendments retain the 30-day cure period, but remove the AG notification requirement.

WILL CCPA ENFORCEMENT EFFORTS BEGIN ON THE JANUARY 1, 2020 OPERATIVE DATE?

The CCPA Amendments do not alter the Act's original January 1, 2020 operative date. As noted above, however, the CCPA Amendments extend the deadline for the AG to publish implementing regulations. Additionally, the CCPA Amendments change the AG's enforcement action start date to July 1, 2020 or six months after publication of the final regulations, whichever date is earlier.

The simultaneous delay in enforcement and extension of the AG's rulewriting deadline create uncertainty on the timing of potential AG enforcement actions. If the AG publishes the final regulations:

- Before June 30, 2019, enforcement actions could start on January 1, 2020.
- Between July 1, 2019 and December 31, 2019, enforcement actions could start sometime between January 1, 2020 and July 1, 2020, depending on the exact publication date.
- Between January 1, 2020 and July 1, 2020, enforcement actions could start on July 1, 2020, potentially leaving businesses with little or no time to comply with the published regulations.

Ultimately, businesses should not wait on the AG to publish final regulations to begin compliance efforts or count on July 1, 2020 as the "go" date for AG enforcement.

Moreover, consumers may begin to make requests under the CCPA, and sue under the statute's narrowed private right of action on January 1, 2020.

CAN THE FEDERAL GOVERNMENT PREEMPT THE CCPA OR OTHER STATE LEGISLATIVE PRIVACY EFFORTS?

As a theoretical matter, Congress certainly could enact legislation that creates nationwide privacy standards and expressly preempts the CCPA and any other state laws establishing privacy rights.

As a practical matter, however, the likelihood of a federal privacy regime (at least in the short term) seems low. After more than a decade of attempts, Congress has failed to enact federal data security and breach notification standards. While the CCPA will energize industry efforts to lobby for exclusive federal privacy standards, the level of congressional interest in tackling this issue is unclear, as is a template of what appropriate federal legislation might look like.

Nonetheless, many businesses will likely prioritize this issue in their government affairs agendas in 2019.

MUST CERTAIN BUSINESSES COMPLY WITH BOTH THE CCPA AND SECTOR-SPECIFIC PRIVACY LAWS? WHAT HAPPENS IF THE CCPA CONFLICTS WITH THIS TYPE OF LAW?

Businesses may be subject to both the CCPA and sector-specific laws. However, the CCPA excepts from its coverage certain information protected or governed by specific federal privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Driver's Privacy Protection Act (DPPA). It also excepts from its coverage certain information that is protected and governed by specific California privacy laws, such as the Confidentiality of Medical Information Act (CMIA) and the Financial Information Privacy Act (SB1).

The CCPA originally contained ambiguities about the scope of the various exceptions. The CCPA Amendments address certain ambiguities and alter the CCPA's original exceptions by:

- Expanding the scope of the HIPAA exception to apply to protected health information that both HIPAA covered entities and business associates collect.
- Providing that the CCPA does not apply to a health care provider's patient information or a covered entity's patient information, if the provider or entity maintains it in the same manner as medical information subject to the CMIA or protected health information subject to HIPAA.
- Adding a new exception for certain clinical trial information.
- Removing the CCPA's original "in conflict" qualification that limited the scope of the GLBA and DPPA exceptions to the extent the CCPA was "in conflict" with those statutes.
- Further expanding the GLBA exception to cover information collected, processed, sold, or disclosed pursuant to California's parallel financial privacy law, SB1.

These expansions aside, the GLBA, SB1, and DPPA exceptions do not apply to the CCPA's private right of action. That is, notwithstanding the exceptions, the CCPA grants a consumer the right to sue for certain data security incidents that may involve personal information covered by those statutes.

For more on the CCPA and the CCPA Amendments, see Legal Updates, California Enacts Consumer Privacy Act of 2018 (W-015-5200) and California Amends the Consumer Privacy Act of 2018 (W-016-7516). For more on California's privacy and data security laws in general, see Practice Note, California Privacy and Data Security Law: Overview (6-597-4106).