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

PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

Search the Resource ID numbers in blue on Westlaw for more.

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.

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 will impose significant obligations and restrictions on many businesses that handle the personal information (PI) 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 California's rapid passage of the CCPA and how business should start preparing for its January 1, 2020 effective date.

WHO DOES THE CCPA PROTECT?

The CCPA protects "consumers," which it defines as California residents. This means that the CCPA applies to PI relating to any California resident, regardless of a business's relationship to the individual.

WHO MUST COMPLY WITH THE CCPA'S REQUIREMENTS?

The CCPA applies to any entity that collects PI relating to California residents, determines the purposes and means of processing of the PI, 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 PI relating to 50,000 or more consumers, households, or devices.
- Derives 50% or more of its annual revenue from selling consumer PI.

WHAT QUALIFIES AS PERSONAL INFORMATION?

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

The PI definition also includes, but is not limited to, 11 enumerated categories of information relating to consumers. Several of those categories contain information that US privacy laws do not typically reference in PI definitions, such as:

- Commercial information, including purchasing or consuming histories or tendencies.
- Internet activity, such as browsing patterns, search history, or a consumer's interaction with a website, application, or advertisement.
- Inferences drawn from any of the enumerated categories of PI.

While the CCPA defines PI in detail, the definition's reference to information linked to a particular household, which could include any child, spouse, or even roommate, creates uncertainty regarding its scope.

WHAT ARE THE COMPLIANCE REQUIREMENTS?

The CCPA imposes a number of obligations in connection with the individual rights the CCPA creates for consumers:

- **Right to Deletion.** Businesses must delete—and direct service providers to delete—any PI collected about a consumer who submits a verified deletion request. The CCPA includes nine exceptions to this requirement, which will need to be carefully considered when implementing procedures to comply with a consumer's deletion request.
- **Right to Access and Portability.** Businesses must disclose in response to a verified consumer request:
  - categories of PI collected;
  - categories of PI sold to a third party;
  - categories of PI disclosed for a business purpose;
  - categories of third parties to whom the business sold or disclosed PI for a business purpose;

  - the business or commercial purpose for which PI was collected or sold;
  - the categories of sources from which PI was collected; and
  - the "specific pieces" of PI a business collected about an individual.
- Businesses must provide this information as it relates to PI 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."
- **Right to Opt Out.** Businesses must enable and honor consumer requests to opt out of the sale of PI. For consumers ages 16 and under, businesses must obtain express consent to sell PI.
- **Right to be Free from Discrimination.** Businesses cannot charge different prices or rates to consumers, provide different services, or deny goods or services to consumers who exercise their rights under the CCPA. There are exceptions to this requirement, and the CCPA also allows businesses to offer financial incentives to collect, sell, or not delete PI.

Businesses must disclose these rights to consumers in their privacy policies and any California-specific description of consumers' privacy rights, as well as list the categories of PI that businesses collected, sold, or disclosed for a business purpose within the last 12 months. To help consumers easily exercise their "opt out" rights, businesses must also include a "Do Not Sell My Personal Information" link, for example, on their homepages.

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

Each covered business will have to decide whether to extend the CCPA's privacy rights to non-California residents. A number of practical and competitive considerations impact this decision, including:

- Whether the business can easily and effectively distinguish between information relating to California residents and information relating to residents of other states.
- The impact on customer relations of telling non-California customers that they do not have the same privacy rights as California customers.
- The legal risks associated with voluntarily making privacy-related representations to consumers throughout the US and thus 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.

It is possible that given the steps businesses will need to take to comply with the CCPA that it may make operational sense for businesses to implement nationwide procedures. But businesses will need to think through various considerations, including those above, as well as how, if at all, they can distinguish between California and non-California residents in complying with the CCPA.

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

Businesses will need to be compliance-ready by the CCPA's January 1, 2020 effective date. While regulations will be forthcoming that will impact compliance efforts (along with, potentially, legislative amendments), there are some immediate steps that businesses should consider, both for compliance purposes and to determine key areas for advocacy:

- **Track data streams.** To respond to consumer requests and update privacy policies, businesses will need to know:
  - when and how they collect PI about California residents;
  - where they store that information and for how long; and
  - with whom they share that information.
- The CCPA defines PI broadly, so fully canvassing how the business handles consumer PI becomes important.
- **Identify operational challenges that compliance may pose.** Consider what systems and processes need to be in place to implement the deletion, access, portability, and opt out requirements and consider which aspects of those requirements are the most burdensome (or even impossible). This will help inform advocacy efforts to amend the CCPA's most onerous or ambiguous provisions.
- **Develop processes to enable compliance.** Businesses 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, and designating an individual to monitor and respond to requests;
  - verifying the identity and authorization of consumers making access or deletion requests;
  - designating individuals to respond to requests within 45 days;
  - setting up mechanisms to honor opt out requests and obtaining consent to sell PI for consumers under 16; and
  - updating privacy-related disclosures, such as online privacy policies.
- **Consider alternative business practices.** Consider whether and how to change handling of consumer PI given the CCPA's requirements as well as explore options under the anti-discrimination provision of the CCPA, including alternative pricing models and financial incentives to offer to consumers relating to the collection, sale, and deletion of their PI.

IS THIS A LAW THAT THE FEDERAL GOVERNMENT COULD PREEMPT? WHAT WOULD A FEDERAL LAW THAT PREEMPTS THIS STATE LAW LOOK LIKE?

As a theoretical matter, Congress could enact legislation that creates nationwide privacy standards and expressly preempts the CCPA or any other state laws that are passed in California's wake. As a practical matter, however, the likelihood of federal preemption (at least in the short term) is low. Despite more than a decade of attempts, Congress has failed to enact federal data security and breach notification standards. And while the CCPA will energize industry efforts to lobby for exclusive federal privacy standards, Congress' interest in tackling this issue—as well as what appropriate federal legislation would look like—is unclear. Nonetheless, the issue will likely play a significant role in the Congressional government affairs agendas and priorities for many companies in 2019.

WHAT IS THE SIGNIFICANCE OF THE JANUARY 2020 EFFECTIVE DATE? WILL ENFORCEMENT START THEN?

Businesses must be ready to comply with the CCPA when it goes into effect on January 1, 2020. Consumers will likely begin making requests under the law immediately after it goes into effect, and some may seek to test the CCPA's private right of action for general violations soon thereafter.

WHAT ABOUT BUSINESSES COVERED BY SECTOR-SPECIFIC PRIVACY LAWS LIKE THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA), THE GRAMM-LEACH-BLILEY ACT (GLBA), OR CALIFORNIA'S CONFIDENTIALITY IN MEDICAL PRACTICES ACT? DO THEY NEED TO COMPLY WITH BOTH THE CCPA AND THEIR SECTORAL LAWS? WHAT HAPPENS IF THEY CONFLICT?

The CCPA includes several exceptions based on specific federal privacy laws, including HIPAA, the GLBA, the Fair Credit Reporting Act (FCRA), and the Driver's Privacy Protection Act (DPPA). In general, however, these exceptions are focused only on information subject to or otherwise handled pursuant to these specific laws (as opposed to entities subject to those laws). As a result, even if broadly construed, the exceptions would not apply to information about California residents that is not covered by these federal laws.

More importantly, several exceptions, including the GLBA and DPPA exceptions, apply only to the extent the CCPA conflicts with the federal standards. The term "conflict" could be interpreted narrowly to mean that a business is unable to comply both with the CCPA and the federal standards as a result of a conflict. If interpreted narrowly, these exceptions may not provide meaningful relief unless a court concludes there is, in fact, a conflict. Because the CCPA creates new privacy obligations not covered in these laws, like the right to deletion, it is possible that courts would not find an actual conflict.

THE LAW REQUIRES THE ATTORNEY GENERAL TO SOLICIT BROAD PUBLIC PARTICIPATION TO ADOPT RELEVANT REGULATIONS. WHAT TYPES OF REGULATIONS DO YOU THINK ARE ON THE HORIZON? WHAT TYPES OF BUSINESSES DO YOU THINK SHOULD OFFER COMMENTS OR PARTICIPATE?

The CCPA gives the California Attorney General (AG) authority to adopt regulations to further the CCPA's purpose as needed and specifically requires the AG to adopt regulations by June 28, 2019 regarding the CCPA's:

- Opt out provisions.
- Notice provisions.
- Access and portability provisions.
- Exceptions necessary to comply with state and federal laws.

The AG may, for example:

- 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, or portability requests.

The CCPA also requires the AG to adopt other regulations, such as adding categories of PI to address changes in technology, data collection, obstacles to implementation, and privacy concerns, on or before the CCPA's January 1, 2020 effective date.

The CCPA applies broadly across industries, and it will be important for businesses across industries to participate in the rule-making process.

For more on the CCPA, see Legal Update, California Enacts Consumer Privacy Act of 2018 (W-015-5200). 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).

PURVI G. PATEL

Purvi G. Patel is a partner in Morrison & Foerster's Los Angeles office and a member of the firm's Consumer Litigation and Privacy & Data Security practices. She defends and counsels retail, technology, e-commerce, and other businesses in significant advertising, unfair competition, consumer fraud, and privacy matters. She can be contacted at ppatel@mofo.com.

NATHAN D. TAYLOR

Nathan D. Taylor is a partner in Morrison & Foerster's Washington, D.C. and Northern Virginia offices and a member of the firm's Banking & Financial Services and Privacy & Data Security practices. He advises organizations on enhancing their cybersecurity posture and preparedness. He can be contacted at ndtaylor@mofo.com.

ALEXANDRA E. LAKS

Alexandra E. Laks is an associate in Morrison & Foerster's San Francisco office and a member of the firm's Privacy & Data Security and Litigation practices. She can be reached at alaks@mofo.com.

07-18