Data privacy enforcement on the rise in the US – California's CCPA setting the benchmark

August 19, 2019

On January 1, 2020, California will become the first state in the US to implement a sweeping new data privacy law that gives its residents the right to know (1) what "personal information" has been collected about them; (2) with whom it has been shared; (3) how it may be deleted; and (4) how to stop it from being sold. Known as the California Consumer Privacy Act of 2018 (CCPA), the new regime signals a significant shift in US privacy law and will greatly impact how covered businesses collect, use, store and share the "personal information" of all California residents, including non-consumers, job applicants, employees and business-to-business partners.

The CCPA is expansive in scope, both in terms of substance and enforcement. It applies extraterritorially; covers new forms of data such as IP addresses and internet browsing activity; defines "sale" broadly to include the exchange of "personal information" for not only monetary consideration, but for any "valuable" consideration; and provides for both regulatory enforcement and a private right of action. With just under four months until the law takes effect, covered organizations are working hard to understand the complexities of the new law and build CCPA-ready compliance programs. Some are updating existing corporate compliance programs, including programs built in response to last year's European Union General Data Protection Regulation (GDPR), while others are building programs from scratch. But no matter the organization's posture, all entities are asking the same question: What does CCPA compliance look like?

Unfortunately, the CCPA does not provide a roadmap for compliance. Although certain provisions of the Act require covered businesses to update their external facing privacy notices with certain language and links, there are no express requirements for internal facing policies and procedures, risk management, or accountability. From a compliance perspective, it's somewhat of a blank slate. It's therefore important to look outside the box for guidance.

In April 2019, the Criminal Division of the US Department of Justice (DOJ) released an updated guidance document for white-collar prosecutors to use in the evaluation of corporate compliance programs. "The Evaluation of Corporate Compliance Programs" sets forth topics the Division has found relevant in evaluating corporate compliance programs in the course of criminal investigations and potential actions thereafter. Several sections of the guidance document are directly relevant to the building of a CCPA-focused compliance program, including the incorporation of risk assessment into the process, developing robust internal facing policies and procedures, implementing training, and ensuring third parties are managed effectively.

Below we provide an overview of the CCPA, outline its various components, and offer five compliance tips through the prism of the DOJ's 2019 guidance that organizations can take now to get ready for the CCPA in January.

CCPA Overview

Who is covered?

The CCPA applies only to a covered "business," which the Act defines as any for-profit entity that: (1) does business in California; (2) collects or determines the "purposes and means of the processing" of a California resident's "personal information"; and (3) satisfies one of the following three thresholds:

- Gross revenues in excess of US$25 million;
- Buys, receives, sells or shares the personal information of 50,000 or more California residents, households or devices in a year; or
- Derives 50 percent or more of its annual revenues from "selling" consumer personal information.

A "business" is also defined as any for-profit entity that controls or is controlled by a business as defined above and that "shares common branding with the business."

"Consumer" defined

The CCPA broadly defines "consumer" to mean any natural person that is a California resident (as defined under California law) "however identified, including by any unique identifier." The phrase "unique identifier" is also broadly defined. The definition of "consumer" therefore ostensibly includes job applicants, employees, non-consumers, business-to-business partners, officers, directors and competitors. An amendment is pending that would exclude job applicants, employees, directors and officers.

"Personal information" defined

The CCPA's definition of "personal information" is equally expansive. The Act defines "personal information" that which "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 provides the following (non-exhaustive) list of examples of personal information:

- **Identifier information**, such as real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, signature, physical characteristics or description, telephone 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, or other similar identifiers;
- **Characteristic information**, such as race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status;
- **Commercial information**, such as records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies;
- **Biometric information**, such as fingerprint, iris scan, or geometric outline of face or body;
- **Internet or electronic network activity information**, such as browsing history, search history, and information regarding a California resident's interaction with an internet web site, application, or advertisement;
- **Geolocation information**, such as the location of the particular consumer or household;
- **Audio, electronic, visual, thermal, olfactory, or similar information**;
- **Professional or employment-related information**;

- **Education information**; and
- **Inferences drawn from any of the above** to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.

Summary of new rights and obligations

Right to disclosure and duty to disclose

The CCPA gives California residents the right to demand, through a verifiable consumer request, that a business disclose the categories and specific pieces of personal information about the resident that it has collected, sold or disclosed in the preceding 12 months. Businesses, in turn, must timely respond to such requests (i.e., within 45 days of receipt, unless extended). Businesses must also disclose "at or before the point of collection" the categories of personal information collected and the purposes for use about California residents, and must include on external-facing privacy notices a description of the consumer's right to disclosure and a list of the categories of personal information the business has collected, sold or disclosed for business purposes in the preceding 12 months.

Right to opt-out and duty to notify

The CCPA also gives California residents the right to "opt-out" of the "sale" of their personal information. The word "sale" is defined broadly to mean any exchange of personal information for monetary or other valuable consideration. Businesses must provide California residents notice of their opt-out right and the potential for any sale of their personal information, and include on their home page a "clear and conspicuous link" titled "Do Not Sell My Personal Information" which, when activated, will allow California residents to opt-out. Businesses must also include a description of the new right on their external-facing privacy notices, train all individuals responsible for handling opt-out requests, and respect the consumer's decision to opt-out for at least 12 months before requesting another sale of their personal information.

Right of deletion and duty to delete

The CCPA also gives California residents the right to request that a business delete their personal information, subject to certain exceptions. Upon verification of the request, businesses will be obligated to delete that information and direct any of their "service providers" to do the same.

Risk of non-compliance

The risk of CCPA non-compliance can be significant. The state Attorney General has the sole authority to enforce the entire CCPA and to impose civil penalties of $2,500 per violation (or $7,500 for each intentional violation). And unlike the GDPR, there are no caps on civil penalties. Businesses may also seek advisory guidance from the state Attorney General (a provision the AG's office has sought to write out of the law through amendment). The state AG is also scheduled to release draft implementing regulations in the fall. California residents also play a role in enforcement, and may bring a private right of action against any business that suffers a negligent data breach as a result of its "violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Such suits may include requests for injunctive relief and/or statutory damages in the amount of $100 to $750 per consumer, per incident, or "actual damages," whichever is higher.

DOJ guidance overview

Although the state Attorney General has not released compliance guidance, it's helpful to leverage the DOJ's April 2019 guidance on corporate compliance when thinking through compliance structures under the CCPA. The DOJ's April 2019 guidance, which is meant to assist US prosecutors in making informed decisions as to whether, and to what extent, a corporation's compliance program was effective at the time of a criminal offense. The guidance highlights three guiding questions for any corporate compliance program review:

- Is the corporation's compliance program well designed?
- Is the program being applied earnestly, in good faith and effectively?
- Does the program work?

In terms of design, the DOJ recommends that a corporate compliance program include an adequate risk-assessment structure, policies and procedures, training and communications, a confidential reporting structure and investigation process, and third-party management.

Tip No. 1: Align strategy and data mapping

Before an organization begins to plan for the CCPA, it should first determine its overall data privacy/information security strategy. This strategy determination will drive the organization's compliance efforts and, as the DOJ recommends, help the organization allocate appropriate resources to the data privacy/information security function. It will also help the organization design a risk management program that adequately identifies, assesses and defines the organization's risk profile.

Consider, for example, a business that operates in 25 US states, including California, and uses a single online privacy policy for all of its states and websites. In its current privacy policy, the business does not extend the rights of disclosure, deletion or opt-out of the sale of personal information. In preparing for the CCPA, should the business adopt the CCPA's new data privacy rights across all jurisdictions, or create a carve-out program for California only? How should the organization handle varying definitions of "personal information" across multiple jurisdictions? On the one hand, adopting California's progressive approach to data privacy across the organization could be useful in mitigating against future changes in the laws of other jurisdictions (e.g., state copycat laws) or in federal data privacy law. It could also be used as a market differentiator. On the other hand, offering data subject rights in jurisdictions where no such rights currently exist will likely increase the business's liability exposure. Determining the appropriate data privacy/information security strategy in light of the organization's risk tolerance is therefore a critical first step to CCPA compliance.

Equally important is undertaking a data mapping/data inventory exercise. This step is particularly important under the CCPA because the definition of "personal information" under the Act is so broad that data points not previously considered sensitive (e.g., IP address, internet browsing activity, etc.) now must be treated as personal information. Only by undertaking a data mapping/data inventory exercise can an organization appropriately understand and appreciate its risk profile and the degree to which it should devote scrutiny and resources to its compliance program.

Tip No. 2: External- and internal-facing notices, policies and procedures

A well-designed compliance program includes policies and procedures that give content and effect to the organization's risk assessment process. According to the DOJ, such policies and procedures should flesh out "ethical norms" and "address and aim to reduce risks identified by the company as part of its risk assessment process." The CCPA requires covered businesses to update and change their external-facing privacy notices. It also will force

organizations to update and change their internal-facing policies and procedures, or create new ones. For example, an organization receiving consumer requests for disclosure, deletion or to opt-out of the sale of the personal information will need to be prepared to receive those requests, verify the identity of the requesting party and respond within the time frame specified under the law (i.e., within 45 days from the date of the request for a disclosure, unless an appropriate extension applies). Organizations that receive a request for deletion will also need to be in a position to verify whether the information is subject to an appropriate exception; whether any of its service providers have the same information (and must therefore be directed to delete); and whether any other exception applies to the California resident's request. Developing robust policies, procedures and notices is therefore a critical step in preparing for the CCPA.

Tip No. 3: Training

Another hallmark of a well-designed compliance program, according to the DOJ, is appropriately tailored training and communications. This includes taking steps to ensure that policies and procedures are integrated into the organization; that critical information is relayed in a manner tailored to the audience's size, sophistication, or subject matter expertise; and that appropriate personnel are trained in carrying out the procedures dedicated to mitigating the organization's risk. The CCPA contains some express training requirements (e.g., personnel handling opt-out requests). Organizations would also be wise to implement comprehensive CCPA and privacy/security training; audit that training; and ensure that communications concerning CCPA requests are uniform and easily understood throughout the organization.

Tip No. 4: Third-party risk management

The DOJ states that a well-designed compliance program "should apply risk-based due diligence to its third-party relationships." This includes understanding third-party partners' qualifications, associations, reputations and relationships; ensuring that they have appropriate controls in place; and understanding how those third-party relationships are managed. Third-party risk management is especially important for CCPA compliance because the transfer of personal information to service providers is exempt from the opt-out rights. "Service provider" is narrowly defined as any entity that "processes information on behalf of a business" and to which the business discloses a California resident's personal information for a "business purpose" pursuant to a written contract, provided that the written contract "prohibits the entity receiving the information from retaining, using, or disclosing" the personal information for any other purpose than specified in the underlying contract. Determining the existence and scope of third-party relationships, and having a firm understanding of service provider relationships, is therefore a key function of CCPA compliance. It is also important because the security posture of service providers may impact the liability of the covered business when there is a private right of action brought by a California resident following a data breach.

Tip No. 5: Information security audit

The private right of action under the CCPA currently applies only if a California resident's non-encrypted or non-redacted personal information is compromised or breached as 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 to protect the personal information." Although the law does not define the phrase "reasonable security procedures and practices," many organizations currently rely on federal or international standards as a benchmark for "reasonable" information security. But those standards vary. One company may track its information security practices with the so-called "NIST" standard (a widely accepted 2014 cybersecurity framework prepared by the US Department of Commerce's National Institute of Standards and Technology). Another may track the international security standards created by the International Standards Organization. Or companies may follow industry-specific standards, such as the Common Security Framework (CSF) established by the Health Information Trust Alliance (HITRUST), or frameworks for critical infrastructure, such as the US Transportation Service's Pipeline Security Guidelines or the

North American Electric Reliability Corporation's Critical Infrastructure Protection (CIP) standard.

California may have its own information standards, separate from federal, international or industry-specific standards. In the "2016 California Data Breach Report," then state Attorney General Kamala Harris expressly endorsed the Center for Internet Security's Critical Security Controls as a "reasonable" security measure, stating that they "define a minimum level of information security that all organizations that collect or maintain personal information should meet," and that "[t]he failure to implement all the Controls that apply to an organization's environment" would constitute a "lack of reasonable security." As the CCPA moves toward implementation, covered businesses should conduct a gap assessment of their current information practices to ensure they are operating within the appropriate framework.

Looking ahead

There is no one-size-fits-all solution for CCPA compliance. Because the law does not provide a clear roadmap for compliance, each organization will need to look at the CCPA requirements through the lens of its own risk tolerance and compliance structure. Third-party risk and gap assessments, preferably conducted through a law firm to maintain privilege and protection, are a good first step. And, of course, all these efforts may need to be revisited as the California State Legislature adopts substantive amendments (scheduled to be complete by September) and the state Attorney General releases its anticipated implementing regulations this fall (estimated for October).

In the interim, organizations should plan and develop a CCPA compliance program, remain flexible over the next few months, and think strategically about how they want to be viewed and to position themselves on issues of data privacy and information security across the enterprise and in their respective markets.

If you have any questions concerning CCPA compliance, please do not hesitate to get in touch with one of the key contacts.

Your Key Contacts

Todd D. Daubert
Partner, Washington, DC
D +1 202 408 6458
M +1 202 436 1819
todd.daubert@dentons.com

Stephen L. Hill, Jr.
Partner, Kansas City
D +1 816 460 2494
stephen.hill@dentons.com

Peter Stockburger
Partner, San Diego
D +1 619 595 8018
peter.stockburger@dentons.com