Hazard Ahead! The Surprising Reach of the California Consumer Privacy Act

The California Consumer Privacy Act (CCPA), enacted earlier this year, will drive class action lawsuits for information breaches as well as impose sweeping new compliance obligations on any company doing business in California that collects or uses personal information about California residents (including employees). The CCPA has been called the U.S. GDPR; but while some of its requirements are similar, the CCPA applies to a much broader data set than GDPR or any U.S. privacy law to date. For most consumer-focused industries outside of financial and health services, the CCPA will be a game-changer—the first direct regulation of online and offline information practices—imposing costly compliance burdens, and significant enforcement and litigation risks. Here is what you need to know to navigate the CCPA's long and winding road.

The CCPA Will Impact Nearly Any Company Doing Business in California

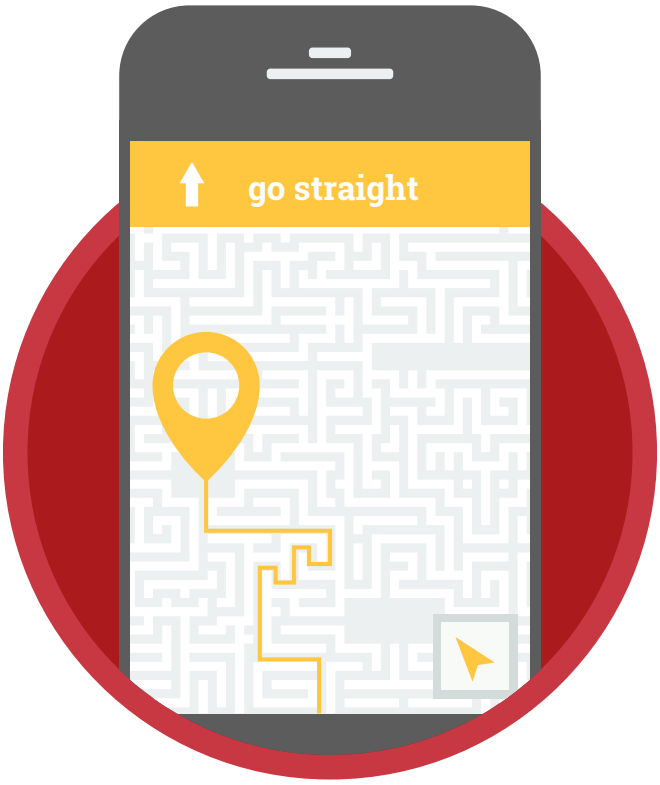
The CCPA applies to a host of businesses that have not been subject to specific privacy requirements in the past, even those with a relatively small California presence. Specifically, the CCPA will apply to any for-profit entity doing business in California that collects personal information and:

> Has gross revenues of more than $25 million;
>
> Annually receives, sells, or shares the personal information of 50,000 or more California residents/employees, households, or devices; or
>
> Derives 50% or more of annual revenues from selling personal information.

Most consumer businesses with an online presence will meet the threshold of annually receiving information on 50,000 individuals, households, or devices. The inclusion of "devices" in this context is particularly significant, because physical presence of a device in California does not necessarily mean it belongs to a California resident, and vice versa, a device detected outside California could nonetheless belong to a California resident who is traveling out of state. Muddying the field further, while a person has to be a California resident in order to qualify as a consumer, the definition of device is not tied to California, and household is undefined. (The broad definition of personal information is discussed below.) Further, the statute applies to any entity doing business in California that meets either of the two revenue-based criteria, regardless of whether that revenue is derived from California residents.

The CCPA Reaches Nearly Every Type of Data Capable of Association with a Consumer or Household

The statute's definition of "personal information" is extremely broad; it includes any information that "is capable of being associated with . . . a particular consumer or household." The statute provides examples of personal information that include "purchasing or consuming histories or tendencies" and "information regarding a consumer's interaction with an Internet web site, application, or advertisement." The statute also includes "audio, electronic, visual, thermal, olfactory, or similar information" capable of being associated with a consumer or household. As a result, even information collected by a business solely for internal use is subject to the CCPA—including any data related to a California resident employee.



Businesses Must Disclose Personal Information to the Consumer On Request

If the CCPA applies to your business, it will impose a significant and unavoidable compliance burden. The CCPA requires businesses, upon receipt of a verifiable request, to provide the specific personal information the business has collected about the requestor over the previous 12 months. Compiling all data "capable of being associated with" a California resident or household – encompassing both online and offline sources– poses operational challenges, particularly in the case of unstructured data stores.

The verified request requirement also presents unique challenges. Most businesses that engage with consumers do not have the ability to verify that a request actually is from a specific consumer and not an imposter. In addition to the compliance burden, this scenario also provides a ready-made portal to facilitate class action lawsuits based on unauthorized access to personal information.

The CCPA Provides Rights to Delete and Opt Out of Sale of Personal Information

Under CCPA, California residents also have the right to request deletion of personal information collected from them, subject to broad exceptions. For example, businesses are permitted to retain personal information that is necessary for internal uses aligned with consumer expectations and the consumer's relationship with the business, and for other internal uses "compatible with context in which the consumer provided the information." California residents also may opt out of the sale of personal information to third parties. This opt-out right, however, does not restrict the business's own, or its service providers', use of personal information.

The CCPA May Put the Brakes on Some Loyalty Programs and Data-For-Service Offerings

The impact of some provisions may prove particularly onerous for consumer loyalty programs and other data-for-service offerings, including some ad-supported services. The statute prohibits businesses from using discounts, or offering differing quality of goods or services, to discriminate against a consumer based upon the exercise of rights under CCPA—unless the price difference is "reasonably related to the value provided to the consumer by the consumer's data." As a result, loyalty program discounts that rely on the exchange of personal information between businesses must be able to calculate the value a consumer receives from participation in the program relative to the value of that consumer's data. The appropriate criteria for determining these "values" is unclear. Accordingly, businesses subject to the CCPA should exercise great care in structuring any loyalty programs that rely on the exchange of personal information with third parties.

Unencrypted Personal Information Now a One-Way Street to Class Action Litigation

While the majority of the CCPA provisions can be interpreted, and enforced, only by the California Attorney General, the statute provides consumers with a private right of action for unauthorized access to unencrypted personal information. The statute only requires a showing that the breach resulted from the business's failure to maintain reasonable security practices and procedures. The CCPA does not explain what "reasonable" practices and procedures are, however. Litigants do not need to show actual damages or specific harm to recover statutory damages up to $750 per consumer/per incident.

The CCPA Will Be Driving into Your Business Sooner Than You Think

The CCPA becomes effective on January 1, 2020. Accordingly, on that date, businesses should be prepared to beginning processing CCPA access requests for information collected since January 1, 2019, as well as opt-out and deletion requests. The California Attorney General is tasked with issuing rules and undertaking enforcement of the statute prior to July 1, 2020. Given the complexity and novel provisions of the statute, businesses that do not start planning now may well be overtaken by the size of the task.

How DWT Helps Clients to Stay Ahead of the CCPA Curve

Let Davis Wright Tremaine's Technology + Privacy and Security practice jump-start your business on the road to CCPA compliance with a **Baseline CCPA Assessment and Customized Action Plan**. Our process begins with an end-to-end Information Risk Assessment of the client's data collection, storage and use practices. This service includes legal analysis of the client's ability to meet key CCPA requirements and a written summary of key compliance gaps, milestones, and tasks, all tailored to your business needs.

For more information please contact:

Nancy Libin | Partner
nancylibin@dwt.com | 202.973.4218

Helen Foster | Partner
helenfoster@dwt.com | 202.973.4223

Rachel Marmor | Counsel
rachelmarmor@dwt.com | 212.603.6401