WELCOME TO THE HOTEL CALIFORNIA: THE CALIFORNIA CONSUMER PRIVACY ACT IS HERE

The CCPA came about because California consumers demanded that they have a say in the proliferation of their data, particularly when it is shared or sold to companies where they do not have a relationship. To circumvent a ballot initiative championed by a group of California consumers, the California legislature created a law with provisions strong enough to satisfy the consumers, yet able to appease businesses. Nevertheless, the consumers' influence is reflected in the characteristics of CCPA, not previously seen in other privacy laws.

Does the CCPA apply to my company?

If you are wondering if the CCPA applies to your organization, you are not alone. If your business operates in California and collects personal information ('PI') of California residents, their households, or electronic devices, the CCPA will likely apply to you if your organization:

- Has an annual gross revenue exceeding $25 million;
- Buys, receives, sells, or shares PI of 50,000 consumers, households or devices annually; or
- Derives 50% or more of your annual revenues from selling consumers' PI.

The above criteria for the CCPA may exempt small businesses, not-for-profits, and businesses already subject to existing federal laws with consumer privacy protections, such as health care (HIPAA) or financial institutions (GLBA).

DOES the CCPA APPLY TO YOU?* If you check one or more boxes, the answer is likely yes.

- ☐ Do you collect personal identifiers – e.g., email addresses, cookies, phone numbers?
- ☐ Do you engage in transfers of personal / device / household information to a third party?
- ☐ Do you collect electronic network activity data - e.g., browsing history, ad clicks, app usage?
- ☐ Do you collect data from visitors to your websites – e.g., geolocation, IP addresses, Google Analytics?
- ☐ Do you determine the purposes and means of processing personal information?

Do you have a for profit 'California business' with at least one of the following criteria?

- ☐ a) annual gross revenues exceeding $25 million?;
- ☐ b) annually buy, receive, sell, or share PI of 50,000 consumers, households, or devices?; or
- ☐ c) derive 50% or more of your annual revenues from selling consumers' personal information?

**For California resident data*

Effective as of January 1, 2020, the California Consumer Privacy Act (CCPA) is the evolution in privacy protection for individuals.

Notable CCPA Distinctions

- The CCPA has a unique definition of personal information (PI). PI under the CCPA is different than other privacy laws as it has been expanded to include electronic network activity data, household data, and 'inferences'. The CCPA defines 'inferences' used to create a profile about a consumer (i.e., age + motorcycle ownership = risk seeking) as PI, and the business must inform the consumer about it. In addition, information about 'households' is also considered PI, irrespective of whether the information is processed about specific individuals who may live in those households.
- Selling data doesn't just mean selling data for profit; it also includes sharing data. The CCPA includes the 'Right to Opt-out of Selling of Personal information'. Selling is broadly defined to mean selling, renting, releasing, disclosing, disseminating, making available… for monetary or 'other valuable consideration'. This language encompasses the 'selling' of data to another business or third party. Most arrangements could be construed to be of value, as there would be no reason for the 'sale' if the data were not of value to the third party.
- The most unique component of the CCPA, requires 'Do Not Sell My Personal Information', as a link, to be placed on the business' home page. To track and act on the ensuing opt-out requests, the business may have to add new procedures and infrastructure.

I am ready for GDPR - Am I ready for the CCPA?

Although there are some similarities between GDPR and the CCPA, being GDPR compliant will not necessarily prepare you for the CCPA. Taking a closer look:

First, the business must inform the consumer how their PI will be used, prior to data collection (similar to GDPR notice requirements under Articles 13 and 14).

Similar to GDPR's Data Subject Rights, the CCPA has identified 'Consumer Rights' obligations where the business has 45 days to respond to a consumer request. The consumer has a right to know what PI is being collected about them, whether their PI is sold or disclosed, and to whom. They have a right to deletion by the business, and any service providers with whom the business has shared the consumer's PI. This is similar to the GDPR right to be forgotten. The business must allow the consumer to opt-out of the sale of their PI and, unique to the CCPA, ensure that the consumer continues to receive equal service and pricing even if they exercise their privacy rights.

To respond to 'Consumer Rights' requests, businesses will have to know where PI is stored, how it is processed, and with whom it is shared. There are distinct challenges in tracking third parties which may have received a consumer's PI, and it could turn out to be particularly tricky due to the indirect way in which online data is sold, traded, and/or shared. Nonetheless, your organization is responsible for understanding this obligation.

Prepare for privacy regulations not just a single regulation, or two.

Chasing laws and regulations can be a never-ending game if a bottom-up approach is used. Depending upon your business' footprint you could be impacted by state and federal laws along with those that have global implications. Future laws on the federal level are now being discussed in Congress. Attempting to adhere to each individual regulation as a one-off business requirement would be ineffective, inefficient, and costly. The one certainty is that data protection and privacy regulations will continue to be introduced, both in the US and globally, and there could be significant variations between emerging and established laws.

Privacy principles that comprise the core of a holistic privacy program remain constant. A smart organization will not only address the current law, but will prep to get ready for all newcomers with a program that starts by building a flexible privacy foundation by addressing key privacy principles supportive of most regulations. A top-down perspective will allow you to build a manageable, sustainable, compliant privacy program where you can treat everyone's data the same and create one set of compliant rules for all.

CONTACT:

GREG REID
Managing Director,
Data Privacy Leader
greid@bdo.com

ADRIENNE TURNER
Manager, Governance & Compliance
aturner@bdo.com

MEGHAL SAMPLE
Associate, Governance & Compliance
msample@bdo.com

KAREN SCHULER
Principal, National Leader,
Governance & Compliance
kschuler@bdo.com