FTI CONSULTING

COMMITTING TO DATA PRIVACY COMPLIANCE:

THE CALIFORNIA CONSUMER PRIVACY ACT AND STEPS TO PREPARE

California's new data privacy law, The California Consumer Privacy Act of 2018 (CCPA), is ushering in a new era of consumer privacy protections in the U.S. Though still undergoing modifications, the law takes effect January 1, 2020, and will provide broad, GDPR-like privacy protections for California residents. With $2.75 trillion in annual gross domestic product, California's economy is now the fifth largest in the world, meaning that corporations with any level of exposure to U.S. markets likely have a data footprint in California.

The law applies to companies that do business in California and meet one or more of the following:

1) annual gross revenues exceeding $25 million;
2) buys, receives, sells or shares the personal information of 50,000 or more California consumers, households or devices;
3) derives 50 percent or more of its annual revenues from selling consumers' personal information.

> *"Now is the time to assess the impact of the law to your business, understand the obligations and begin taking steps to modify processes accordingly."*

Components addressed and included in the current draft of the CCPA

- **Definition of "sale"**—as the disclosure or availability of personal information for monetary or other valuable gain
- **Inclusion of "household"**—the law's definition remains ambiguous, and may encompass an individual, residence, family, device or group of devices
- **Enhanced privacy notice requirements**
- **The consumer's "right to opt out" of any sale of their data**
- **The individual's right to access**, including the right of disclosure, portability and deletions
- **The right to equal service and prices** (*no retribution or price premiums for "privacy-equipped" services*)
- **Right to be informed of categories of personal information that a business collects, receives, sells or discloses**; purpose of activities; and categories of parties disclosed to
- **New fines enforceable by the California Attorney General**, including civil penalties of up to $2,500 for unintentional violations and up to $7,500 for intentional violations
- **Private rights of action for breach events of nonencrypted or nonredacted personal information**
- **An initial framework for "financial incentive programs"** rewarding consumers that permit the sale of their data

Amendments Approved by Governor on October 11, 2019:

AB 25

A one-year extension for employee data, meaning employee data is exempted from CCPA scope/not treated the same as consumer data until January 21, 2021.

AB 1564

Businesses operating "exclusively online and having a direct relationship with a consumer from whom it collects personal information," receive an exception to the toll-free number requirement; businesses subject to this exception are only required to provide an email address through which consumers can submit data subject access requests.

AB 1355

Includes technical corrections, such as a one-year moratorium on business-to-business communications and exclusion of de-identified and aggregated data from the definition of personal information.

AB 1202

Requires businesses, which collect and sell to third parties the personal information of consumers with whom a direct relationship does not exist, to register as a data broker; annual registration is required, and fines are imposed for any unregistered business operating as a data broker.

Notable Amendments That Did Not Pass:

AB 846

Exemption for loyalty programs from non-discrimination provisions, which would have allowed the collection of personal information for loyalty programs without concerns regarding the non-discriminatory provisions.

AB 2181

If passed, this would have required companies to disclose their use of facial recognition technology; notably, even without this bill, companies are still required to disclose if/when biometric data is collected.

AB 981

Initially aimed at wholly exempting insurers from the CCPA, and later adjusted to provide CCPA exemption for certain insurance transactions and integration of consumer protections in the CCPA with those in other industry regulations.

Areas Worth a Closer Look

Efforts have been made by various parties to both strengthen and weaken the law. With the latest approved amendments, a few key points have emerged as worthy of closer consideration. These include:

Employee data exemption

AB 25 provides only temporary exemption of employee data from CCPA protections. Also, it did not remove the notice provision or private rights of action for employee data. When the amendment expires in 2021, all employee data will be treated the same as consumer data. This gives businesses time to operationalize compliance for employee data, including ensuring that 1) it isn't being sold, 2) opt-out mechanisms are provided and 3) processes for data access requests from current and former employees are enabled.

Inclusion of household

The CCPA's lack of definition for what constitutes a household raises privacy considerations for consumers and businesses. A household may include any combination of an individual, a family, a residence and devices. This creates a complicated web of data that may be associated with any given person. For consumers, it will be difficult to discern how and when a member of the household is authorized to make data requests on their behalf. It will also make business compliance more challenging, as a single data subject request may include obligations to respond across a wide range of data for multiple household members.

Highly regulated industries

Organizations in healthcare, insurance, financial services and other highly regulated industries will need to take additional steps to harmonize compliance between CCPA and regulations such as HIPAA and the Insurance Information and Privacy Protection Act. Compliance with existing regulations does not automatically ensure compliance with CCPA, therefore an understanding of the exemptions, overlap and gaps is critical.

Businesses deemed in scope under the CCPA must:

- Clearly inform the consumer of the personal data they collect and how it is being used
- Provide the consumer with a copy of their personal data if requested to do so
- Allow consumers the opportunity to opt out of the sale of their personal data and avoid requesting opt-in consent for 12 months after an opt-out
- Delete the consumer's data if requested to do so
- Clearly inform consumers of the types of third parties with whom personal data is shared
- Provide the categories of sources of information from whom the consumer's personal data was acquired
- Enable technical safeguards to protect personal data

GDPR Similarities

As many multi-national organizations have already experienced, the EU's GDPR fundamentally changed the way many businesses manage personal data. The CCPA is similar to GDPR in numerous ways, providing privacy rights centered around notice, access and consent for California residents. It will introduce new fines for non-compliance and lawsuit parameters for residents impacted by illegal processing or mishandling of their data.

Organizations that have already implemented privacy-driven changes for GDPR will have a head start. These corporations can take learnings and programs they have deployed in Europe, and apply them to California resident data. But U.S.-based companies that have not dealt with operationalizing data privacy or GDPR compliance will face some heavy lifting to implement the information governance and privacy programs necessary to meet CCPA's requirements.

How to Prepare

To ensure regulatory readiness, there are a handful of steps organizations should take. Key initiatives that can help reduce regulatory, operational and reputational risk, while establishing preparedness for CCPA enforcement, include:

1. Map Your Data

Prepare a clear map of where the organization stores personal data (across digital and hard copies), for how long, and how that data is used or shared with other parties; be sure to include an extensive understanding of the regulatory risk exposure with respect to that data and how the compliance obligations impact products, services, business processes, internal systems, external third-party relationships, etc.

2. Update Privacy Notices

Work with counsel and privacy experts to develop compliant notices that include 1) a description of consumer rights under the law, 2) a comprehensive list of third parties to whom the business sells personal information, 3) categories of third parties to whom the business discloses personal information for business purposes. Privacy notices must be in place by January 2020 for consumers and by January 2021 for employees.

3. Identify and Document Personal Data "Sales"

Provide clear and conspicuous consent requests and a "Do Not Sell My Personal Information" link on your website homepage. Implement a process for handling do not sell requests and make it easy for consumers to navigate. Review vendor contracts to ensure that the sale/use of personal information is limited within the confines of the law, and that data rights requests implicating this information can be responded to and executed in a timely manner.

4. Prepare to Respond to Data Rights Requests

Provide a toll-free telephone number and/or email address where individuals may submit data access requests and/or privacy complaints . Responding to these can require substantial effort. Develop a standardized workflow for fielding requests within the designated 45-day timeline. Prepare an outline for data subject requests that includes authenticating the person(s) making the request and process flow for handling access and deletion of data according to the request. Similarly, have a plan in place for intake and response for privacy complaints.

5. Implement and Commit

Smooth implementation is extremely important, but it can end up in vain if the privacy compliance control environment is not preserved and sustained. Resources and budget must be allocated commensurate to the organization's risk, with separate program resourcing and budget built in to sustain compliance over the long term. Non-compliance comes with a bottom line impact, but so does "over compliance." Taking time to calculate sufficient budget and resourcing, then committing to the spend will help keep privacy program owners accountable to deliver upon the defined risk tolerance. It takes time, material and experienced people to affect data privacy.

FTI CCPA Services Offered

- CCPA "regulatory readiness" assessments
- California consumer data identification and mapping
- CCPA training and awareness
- Subject access request workflow development and execution
- Data monetization strategies
- CCPA incentive program implementation

Remember that these initiatives are a more of a marathon than a sprint. Move forward at a steady pace, taking the process one "mile" at a time. By working proactively and approaching programs in intervals, organizations can better benchmark their progress, and position the organization to cross the finish line successfully, by the time enforcement begins.

FTI Consulting provides a wide range of CCPA services that help reduce our client's regulatory, operational, or reputational risk. From short, project-based engagements to ongoing managed services, FTI Consulting's CCPA services are tailored to each organization's need to ensure regulatory readiness. Our services are provided by a team of data privacy subject matter experts with deep knowledge of municipal, state, national, and global data privacy risk & compliance.

Jake Frazier
Sr. Managing Director
+1 (512) 971-6246
jake.frazier@fticonsulting.com

Chris Zohlen
Managing Director
+1 (415) 307-4956
chris.zohlen@fticonsulting.com

Louise Rains Gomez
Managing Director
+1 (404) 270-1415
louise.rains@fticonsulting.com

Andrew Shaxted
Sr. Director
+1 (773) 658-0241
andrew.shaxted@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT™