Succeeding In The Data Economy: How Companies Can Prepare For CCPA Compliance

By Sandeep Vishnu, Julien Bonnay, Nikita Mehta, Capco
August 13, 2019
ValueWalk

The California Consumer Privacy Act (CCPA), which goes into effect January 1, 2020, signals a major shift in the way that the United States and allied economic powers treat consumer data protection and privacy. For many years, the government's primary focus was protecting data and shoring up authorization practices. This led to multiple innovations in the way of technology and tactics to optimize data access and control. However, it meant that until recently, the government was focused on ensuring authorized access, but was less concerned with regulating usage *after* authorized access.

With CCPA, the United States is aligning more closely with a growing global trend towards better governing the use of data and providing consumers with the ability to determine and direct the use of their data. Coupled with increased regulatory sensitivity toward consumer data, shifting consumer expectations should serve as an early indicator for financial institutions that hardening perimeters and deploying rigorous access control is no longer going to suffice – data element level management and governance is necessary to enable appropriate usage.

Global Shift Toward Governing Data Usage

Governments and regulatory bodies around the world have begun to make strides toward regulating appropriate usage of data to add to existing regulations around safeguarding data. The most restrictive current law in existence is the EU's General Data Protection Regulation (GDPR), a regulation that strengthens and unifies privacy protection across the region and imposes fines upon an organization – up to 4% of the company's annual global revenue – for breaches that occur.

The U.S. has a number of current and proposed laws that parallel this global trend, currently emerging on a state-by-state basis and applying only to companies that do business in that state and/or process data of state residents. At recent count, 14 states had some legislation underway on data protection and privacy, which broadly address four major themes:

- **Data Protection.** Cover, at a minimum, direct information collected about consumers.
- **Transparency and the Right to Know.** What information will be collected about consumers, where it is collected from, why it is being collected, and how will it be shared.

- **Consumer autonomy.** Extend consumers' autonomy over the use of their data.
- Obligations for safeguarding consumer data, including cybersecurity risk management, breach reporting, multifactor authentication, and access limitations.

Eight Steps to CCPA Readiness

As the regulatory landscape shifts towards governing data usage, businesses should begin to integrate privacy into all facets of their business, from internal items like strategy, risk management, and training, to external items like marketing materials for product and service offerings. The major items to consider for any organization are:

1. **Consumer Rights.** Understand and comply with consumer rights: right to know; right to 'be forgotten'; right to opt in/out; and data safeguards.
2. Understand the scope of personal information collected about a consumer – both direct and indirect information about a consumer – business purpose, sources of information, and determine what information is sold or shared to third parties.
3. **Data Management.** Understand what information is collected, why it is collected, and how it flows through organization. Create a methodology to trace information through its lifecycle and define roles for people process and technology.
4. **Policies and Procedures.** Enhance existing policies and procedures to include consumer rights under the CCPA and instructions for how to exercise those rights. Annually review privacy policies to disclose lists of data collected, categories of third parties with whom information shared or sold, and categories of information shared or sold from the prior 12-month period.
5. **Third-Party Risk Management.** Create an inventory of third parties with whom consumer information is shared or sold, classifying third parties versus service providers that may be exempt from certain CCPA obligations. Revise vendor agreements to limit PI data processing outside of the contractual business purpose. Conduct third party audits on service providers who have access to your consumer personal information to ensure compliance with the CCPA.
6. **Risk Management.** Enhance safeguards for consumer data through cybersecurity risk management to ensure that the organization has reasonable security measures. Enhance Monitoring & Testing programs for consumer requests and incident responses.
7. **Servicing Consumer Requests.** Create a customer service request center and processes for consumers to submit requests, and for the organization to intake and respond to request. Businesses have only 45 days to respond to requests. Train all employees on CCPA consumer rights, how consumers can exercise those rights, and how to execute business obligations.
8. Businesses are subject to heavy fines for failure to safeguard consumer data or protect consumer's data rights. Fines under the CCPA are per violation, depending on the type of failure – up to $7,500 for each intentional violation, and $100 – 750 per data breach incident, or actual damages, whichever is greater. The CCPA is progressive in that it gives individuals the right to sue businesses for data breaches.

With breaches on the rise and these privacy laws going into effect early next year, the best way companies can respond is to enable data-element-level management to help defend consumer privacy − and their own − in the data economy.

Article By Sandeep Vishnu, Julien Bonnay, Nikita Mehta, Capco