ESG Brief

California Consumer Privacy Act Overview

Date: December 2019 **Author:** Christophe Bertrand, Senior Analyst & Steve Catanzano, Consulting Analyst

Abstract: The California Consumer Privacy Act (CCPA) goes into effect on January 1, 2020. Often compared to GDPR, CCPA protects consumers from mismanagement of their personal data and gives them control over what data is collected, processed, shared, or sold by companies doing business in California.

The act represents one of the most sweeping acts of legislation enacted by a U.S. state to bolster consumer privacy. Like GDPR, the European privacy act, the California Consumer Privacy Act may be the beginning of stricter U.S. consumer privacy protections.

Overview

The California Consumer Privacy Act is a landmark piece of consumer privacy legislation, which passed into California law on June 28th of 2018. The bill is also known as AB 375. This act is the strongest privacy legislation enacted in any state, giving more power to consumers with regards to their private data.

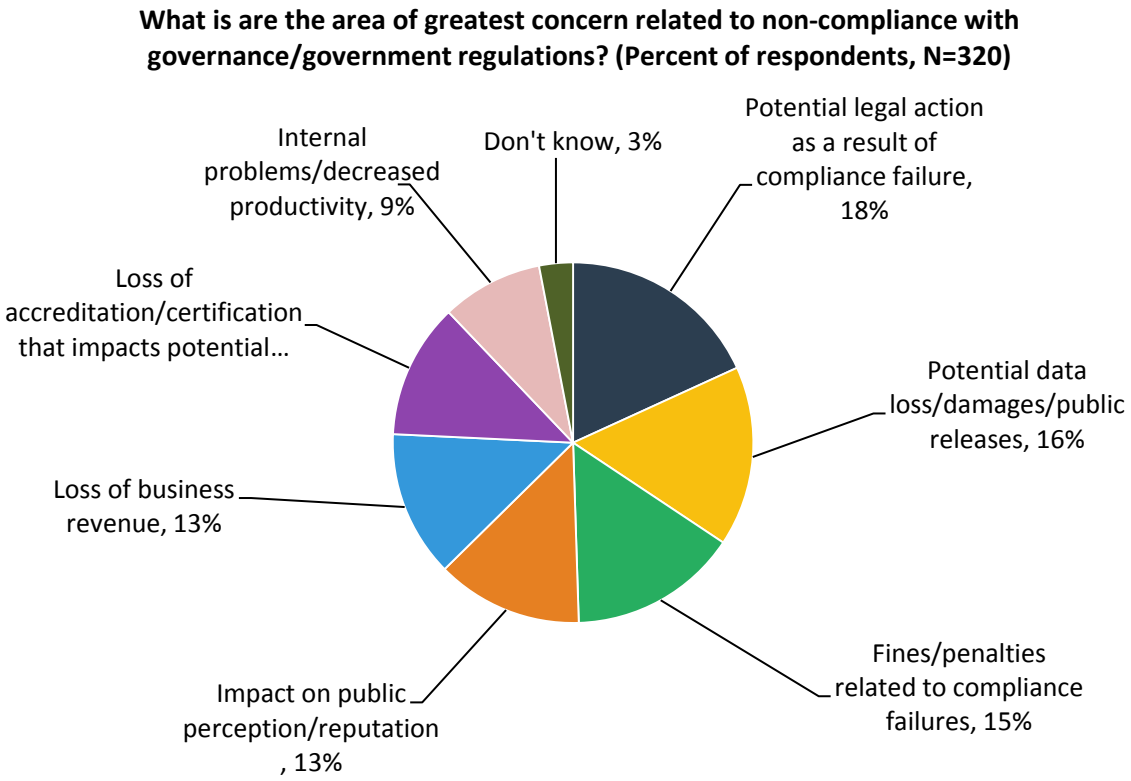
Companies that already comply with GDPR may find that they currently meet many of the requirements set forth in the California Consumer Privacy Act. With many experts predicting that other states will pass similar legislation in the coming years, companies across the U.S. that take proactive steps today to better protect consumer data will be best equipped for future regulations.

These two data privacy regulations fundamentally extend individuals' rights to the data being captured about them, who has it, and how it is used. This also typically includes the ability to have private data deleted or barred from use in certain circumstances. While GDPR is much more prescriptive than CCPA, they both share a notion of protection or preservation of the data that organizations must comply with, for example backups and archives.

Failing to comply with governance/governmental regulations is not an option and can cause many undesirable consequences, as evidenced in ESG research (see Figure 1).[1] The addition of this new breed of data privacy regulations, and in the case of the U.S., the potential multiplication of these regulations, with each state offering its own variation, will only create additional exposures, audits, and risks for those who don't plan accordingly.

[1] Source: ESG Master Survey Results, *2018 Data Protection Landscape Survey*, November 2018.

Figure 1. Impact of Compliance Failures



Source: Enterprise Strategy Group

It should also be noted that neither CCPA (nor GDPR) supersedes other compliance or regulatory requirements (for example, the requirement to keep data archived for x number of years).

Key Terms of CCPA

There are a number of terms defined in the legislation. Certain businesses and all California-resident consumers are the two groups who fall under the provisions in the bill, defined as:

- Consumer: According to the act, "'Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations.
- Business: "Businesses" are defined as any for-profit entities that do business in California and collect personal information of consumers that meets one or more of these criteria:
  - "Has annual gross revenues in excess of twenty-five million dollars ($25,000,000)."
  - "Derives 50 percent or more of its annual revenues from selling consumers' personal information."
  - "Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices."

Defining 'Personal Information'

Another important term loosely defined in the bill is "personal information." According to AB 375, "The bill defines 'personal information' with reference to a broad list of characteristics and behaviors, personal and commercial, as well as inferences drawn from this information."

Dozens and perhaps hundreds of specific data items are mentioned in the legislation, including:

- Biometric data.
- Household purchase data.
- Family information (e.g., how many children).
- Geolocation.
- Financial information.
- Sleep habits.

What Does the California Consumer Privacy Act Provide for Consumers?

- General Disclosure: If a business (as defined by the bill) collects any type of personal information, this should be disclosed in a clear privacy policy available on the website of the business.
- Specific Requests: Should a consumer desire to know what data is being collected, the company is required to provide such information—specifically about the individual. Some of the requests that can be made include:
  - The categories of personal information collected.
  - Specific data collected about the individual.
  - Methods used to collect the data.
  - A business's purpose for collecting the information.
  - Third parties to which personal information may be shared.
  - Deletion: If the consumer desires, personal information (with exceptions) will be deleted by the business.
- Same Service: Regardless of a consumer's request and preferences about how their personal information is handled, businesses are required to provide "equal service and pricing even if the consumer exercises their privacy rights under the Act."

How to Comply with the California Consumer Privacy Act

As it stands, businesses will be required to comply with any and all provisions outlined in the final version of AB 375 by January 1, 2020. Companies actively doing business in California will need to adjust their current practices to avoid violations of the law.

Many of these changes translate to a need for:

- **Organized Data Collection:** The bill allows consumers to request the specific information collected about them. These requests are to be provided at no cost to the consumer. Companies need to have the ability to quickly search, compile, and send these reports to consumers.
- **Clear, Transparent Policies:** Consumers can request a report on the types of data collected, data sources, collection methods, and uses for their data. While the data itself needs to be stored in a well-constructed database, many consumer questions can be quickly answered in comprehensive privacy and data collection policies.
- **Knowledge of Specific Provisions:** There are clearly outlined requirements within the California Consumer Privacy Act, including the need to:
    - "Provide a clear and conspicuous link on the business' Internet homepage, titled 'Do Not Sell My Personal Information,' to an Internet Web page."
    - Ensure that any individuals who handle consumers' private data know and understand all pertinent regulations.

In the time leading up to full implementation in 2020, there will likely be amendments that change current provisions, remove requirements, or even add to the regulation. It is important for all businesses to work towards a safe and healthy relationship between data collection and privacy while staying up to date regarding new data regulations.

The Bigger Truth

A significant number of businesses are not prepared for CCPA and are caught between weighing the cost and effort of complying with the act and the probability of enforcement actions being brought against them. Companies with annual gross revenues of $25 million or more, those that buy or sell more than 50,000 individuals' data, and those that make more than half of their annual revenues from selling customer data need to comply.

For businesses that fail to or refuse to comply, fines can be steep. The CCPA states that companies can be penalized $2,500 for each record of unintentional violation and $7,500 for each record of intentional violation. Ignoring the rules or taking no action to comply may result in intentional violations. This cost is levied per record or instance, meaning fines can rise to the hundreds of thousands of dollars.

Complacency is not a strategy. This is just one of many regulations designed to protect consumers' right to privacy. Organizations should have a comprehensive program, utilizing the right technology partners, to automate their consumer privacy practice and adhere to the regulations. Just as we have seen with GDPR, the companies that fail to make the investment now are only going to have to put in more work and effort down the line.

Organizations need to implement advanced data classification, data anonymization, data masking, security, and access controls in order to set themselves up for successful compliance. ESG believes that many organizations are only ready on the surface—with marketing opt-in/out processes, for example.

Successful organizations must be able, in time, to offer online portals that provide verified users the ability to know all of the data the organizations hold about them, and comply with the various requirements that are applicable.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com P. 508.482.0188