California Consumer Privacy Act

Legislative Changes Needed to Fix Law in 2019

The California Consumer Privacy Act (CCPA) is a sweeping privacy law that applies to businesses of all sizes across almost every industry. It was rushed through the legislative process in the summer of 2018 without the benefit of input from numerous crucial stakeholders. As a result, the law is deeply flawed. Many of the CCPA's provisions are simply unworkable in practice or will result in numerous unintended consequences. At the end of the 2018 session, the Governor signed SB 1121, a bill fixing a handful of the CCPA's problems. However, many more fixes are needed before this law goes into effect on January 1, 2020.

RUSHED PASSAGE OF THE CCPA

In early 2018, a real estate developer named Alastair MacTaggart spent about $3 million of his own money to gather enough signatures to qualify a significantly flawed privacy initiative for the ballot. His initiative was more than 33 pages long, and—had voters approved it—the Legislature would have been virtually unable to amend it in the future. This would have been incredibly problematic because stakeholders from nearly every industry recognized that the initiative had significant deficiencies. The near-impossibility of amendment was particularly troublesome as technology is constantly evolving.

AB 375 (Chau; D-Monterey Park/Hertzberg; D-Van Nuys), titled the California Consumer Privacy Act (CCPA), was introduced as compromise legislation to avert a significant ballot fight in November 2018. Unfortunately, there was only one week from the time the language of the CCPA was introduced to the deadline for MacTaggart to pull the initiative from the ballot. Thus, there was not an opportunity for meaningful stakeholder input. Moreover, MacTaggart would agree to pull the initiative from the ballot only in exchange for the Governor signing a law substantially similar to his ballot initiative, despite its flaws.

The business community opposed AB 375, and yet found itself in an untenable situation because the privacy initiative was even worse. Given the high stakes of fighting the complex and confusing initiative at the ballot box, the business community urged legislators to vote for AB 375 as the lesser of two evils—hoping the Legislature would be able to fix the most egregious problems with the law in the future.

The authors of AB 375 agreed that the CCPA would need fixes. Shortly after it passed, they designated SB 1121 (Dodd; D-Napa) as the vehicle for immediate cleanup of AB 375 and committed to work on bigger problems with the bill during the 2019 session.

The business community assembled a large and diverse coalition of businesses ranging from wineries and movie studios to retail stores and hospitals to propose amendments to fix the numerous flaws with the workability of the CCPA and spent the July 2018 recess poring over AB 375 with privacy experts from around the country. The business community then drafted a detailed letter proposing language for SB 1121 to fix unworkable

CalChamber

California Promise: Opportunity for All

2019 Business Issues and Legislative Guide

See the entire CalChamber 2019 Business Issues and Legislative Guide at www.calchamber.com/businessissues
Free PDF or epub available to download.

Special Thanks to the Sponsors
Of the 2019 Business Issues and Legislative Guide

Premier

Chevron

Silver

AUTOMOBILE CLUB • SOUTHERN CALIFORNIA • AAA

Bronze

enterprise

Iron

Suburban Water Systems
A SouthWest Water Company

Frontier COMMUNICATIONS

aspects of the CCPA and those that would result in unintended consequences. Some of these requested changes were made with the passage of SB 1121. SB 1121 also extended the enforcement date of the CCPA, in part due to a recognition that more needs to be done in 2019.

CCPA APPLIES TO SMALL/MID-SIZED BUSINESSES IN EVERY INDUSTRY

Many people mistakenly believe that the CCPA applies only to "Big Tech." Although the CCPA does apply to large companies in any industry (those making more than $25 million in revenue per year), as well as to data brokers, there is a third, incredibly broad category of businesses—many of them small businesses—often left out of the discussions: **any business that "alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices."**

Personal information for 50,000 consumers may sound like a high number at first blush, but it is not. The CCPA has an incredibly broad definition of "personal information," which includes, for example, IP addresses (a numeric designation that identifies a computer's location on the internet), and the burdensome requirements of the CCPA apply to any business that merely "receives" "personal information" as defined by the CCPA.

Thus, the CCPA applies to businesses with 50,000 yearly website visitors, and this includes ad-supported blogs. It's not a high number. If a business has an average of 137 unique online visitors per day over the course of one year, it will hit the threshold. Businesses that receive 50,000 sales leads in a year must comply with the CCPA, and the same goes for businesses that receive 50,000 consumers' credit card numbers while conducting sales transactions, as well as any businesses that have some combination of consumer personal information. For example, if 25,000 consumers visit a business's website in a year and that business conducts sales transactions with 25,000 different consumers—that company must comply with the CCPA.

The International Association of Privacy Professionals estimates that more than 500,000 businesses are regulated by the CCPA, "the vast majority of which are small-to-medium-sized businesses." Think of all the small businesses that easily conduct an average of 137 transactions per day—or approximately 12 transactions per hour in a 12-hour day—convenience stores, coffee shops, restaurants, tourist kiosks, etc. The CCPA treats these small businesses the same as large tech companies.

WHAT DATA CONSTITUTES 'PERSONAL INFORMATION' UNDER THE CCPA?

Under the CCPA, essentially every piece of data about a person could be classified as "personal information." When most people think of personal information, they think name, birthday, Social Security number, etc.—data that could identify someone.

The CCPA defines "personal information" far more broadly as "information that identifies, relates to, describes, *is capable of being associated with,* or could reasonably be linked, directly or indirectly, with a particular consumer or household."

Basically any piece of data is "capable of being associated with" a particular consumer, and this includes IP addresses as well as "unique identifiers," such as device and cookie IDs, internet browsing history, and characteristics concerning an individual, such as race or sex. This one-size-fits-all approach to personal information is a drastic shift from long-standing policy in California and around the country.

WHO HAS RIGHTS UNDER CCPA?

The CCPA defines a "consumer" as "a natural person who is a California resident." Thus, a "consumer" need not have a customer relationship with a business in order to exercise rights under the CCPA.

WHAT RIGHTS DID CCPA CREATE?

The CCPA provides consumers with the following privacy rights to be enforced by the Attorney General:

- The right to know the categories of personal information a business has collected about them and how.
- The right to access and obtain a copy of their personal information.
- The right to opt out of a business' sale of their personal information.
- The right to request that a business delete their personal information.
- The right to not be treated differently by a business for exercising their rights under the CCPA.

The CCPA also creates a private right of action that massively expands the liability of a business that has been the victim of a data breach. With this private right of action, a consumer does not need to prove any injury and can recover minimum statutory damages of $100 per person, per incident, and a maximum of $750. This unchecked liability will lead to a barrage of shakedown lawsuits, as companies facing such substantial liability will be leveraged into immediate settlement, regardless of the strength of their legal defense.

PROBLEMS WITH CCPA

Following are some of the problems with the CCPA that will lead to unintended consequences:

• Definition of Consumer

As previously discussed, the CCPA defines "consumer" as any California resident. Without clarification, this could be interpreted to include employees, which is problematic for many reasons.

First, the CCPA gives "consumers" the right to request that a business delete their data. If the definition is not changed to exclude employees, an employee accused of sexual harassment could request that complaints about him/her be deleted.

Second, the CCPA gives "consumers" the right to opt out of the selling of their data. This could be problematic when a consumer is both an employee and a customer of a business that sells some data and must, therefore, provide a link to "opt out" on its business website. If that employee/customer opts out, there is nothing in the CCPA that allows the business to distinguish between the data it has on the consumer based on the customer relationship and the data it has on the consumer based on the employment relationship.

In addition, the operational costs of including employees (past and current), job applicants, and other related individuals who do not have a true "consumer" relationship with the business will be exorbitant, and will require many businesses to create separate processes for these individuals.

• Definition of Personal Information

As previously discussed, the current definition of "personal information" is so sweeping as to be meaningless. In theory, every piece of data could be randomly "capable of being associated with" an individual, household, or device. This overly broad definition will undermine existing privacy-protective business practices and impose significant operational costs and burdens on thousands of California businesses.

The definition of personal information should be limited to information that is "linked or reasonably linkable" to a particular consumer. This is consistent with the guidance of the Obama administration's Federal Trade Commission guidance on privacy, and it would make the definition of personal information consistent with the notion of an identifiable individual, as is the case in California's Shine the Light Law, California Online Privacy Protection Act (CalOPPA) laws, and every other privacy law and framework, including the European General Data Protection Regulation (GDPR).

In addition, references to households, families, and devices should be removed from the definition of personal information. As drafted, one member of a household or "family," whether an abusive spouse, a roommate, or a troubled youth, can access any personal information—including credit card information or geolocation information—about another member of the individual's household or family. This runs counter to the privacy goals of the CCPA. Also, the term "device" should be removed because devices often are shared by several people and are not personally identifying. Further, the term "devices" is defined to cover all devices (including even industrial devices) so that the definition far overshoots anything that might identify an individual.

• Specific Pieces of Information

The CCPA requires businesses to provide consumers with "specific pieces of information" the business has collected upon the consumers' request, but does not explain what "specific pieces of personal information" means. It could mean that in response to consumer requests, businesses must transmit incredibly sensitive information, like credit card numbers or birth dates, back to the consumer. This would create unnecessary risks to both the security of the consumer's information and the business's ability to protect such information.

There also is the risk of inadvertent disclosure to a fraudster posing as the consumer because the CCPA forbids a business from requiring any consumer to create an account so the business can verify the consumer requesting his/her data is who they claim to be. Remember, a consumer, as defined by the CCPA, need not have any customer relationship with a business. All of this runs counter to common-sense principles of privacy.

Additionally, despite an exemption in the act that a business is not required to relink or reidentify data, a business cannot provide "specific pieces of information" back to a consumer without relinking or reidentifying data in order to match it to the person making the request.

Requiring a business to maintain records in a form that directly identifies individuals in order to be able to respond to a request for "specific pieces of information" would undermine privacy and these other provisions of the CCPA. In order to facilitate internet commerce while safeguarding consumer privacy and security, businesses typically maintain consumer information in pseudonymized form. This means that information is not directly linked to an identifiable consumer.

Directly linking data contravenes best practices for data security and results in a lower standard of protection for consumer personal information. The CCPA already expands transparency enormously, and this provision is unnecessary from the perspective of increasing transparency and protecting consumers.

• Exemption for Privacy Protective Treatment of Information

The collection, use, retention, sale, and disclosure of

information in deidentified or aggregate or pseudonymized form, where it can be used in place of personally identifiable information, is privacy enhancing and beneficial to consumers because it means that the processing of personally identifiable information about them is reduced. Similarly, businesses that can accomplish their legitimate business purposes through the use of deidentified, pseudonymized, and aggregate information can reduce the amount of personally identifiable information that is subject to potential compromise.

The authors of the CCPA intended a true exemption for aggregated consumer information and deidentified information in order to incentivize businesses to pursue these privacy protective practices. Yet, under the CCPA, for information to qualify as "deidentified," it must not "relate to" or "be capable of being associated with . . . a particular consumer." Unfortunately, those two things are always true of deidentified data, and the term loses all meaning unless it is amended.

In addition to fixing the definition of deidentified so that the exemption for deidentified information can be meaningful, the CCPA should be amended to exempt pseudonymized information as well. Pseudonymization is also a privacy-protective practice that replaces personal identifiers in a set of information with artificial identifiers, or pseudonyms, so that the link to a real identity cannot be established without additional information that is separated from the pseudonymized data.

• Many Other Problems

There are numerous other problems—big and small—with the CCPA that would create unintended consequences for businesses and consumers. Here are just two of the smaller examples:

The CCPA Does Not Allow for Consumer Choice in Opting Out. As drafted, the CCPA mandates only one "all or nothing" opt out. For example, if a consumer opts out of a company selling his/her data to minimize third party marketing, unless the law is clarified, that consumer might also inadvertently be deprived of special discounts and promotions for existing or new services that could save the consumer money. Consumers should have the option to choose the types of sales from which they wish to opt out.

The CCPA Mandates an "Opt-Out" Button on Every Single Webpage of a Website. A drafting error in the definition of "Home Page" defines it as both the home page of a website as well as every web page at which a business collects personal information. The result is to require an "opt-out" button *on every single web page where a business collects any personal information, including an IP address*. Read literally, this would require special California right-to-know notices on virtually every single business web page.

CALCHAMBER POSITION

While the CalChamber appreciates and understands the need and desire for consumer privacy, the CCPA unfortunately has multiple flaws that undermine consumer privacy as well as employee protections. The benefit of the CCPA, as opposed to the withdrawn 2018 initiative, is that the Legislature has time to address these flaws before the entire law goes into effect.

California has the opportunity to lead the country on this issue and produce model legislation on consumer privacy that works for both consumers and businesses. CalChamber will continue to push for crucial legislative changes to fix the CCPA in 2019, and also will be involved in the Attorney General's rulemaking process to ensure that business efforts to implement and comply with the CCPA can be as efficient and safe as possible.

Staff Contact
Sarah Boot
Policy Advocate

sarah.boot@calchamber.com
January 2019