Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress

Wilson C. Freeman
Legislative Attorney

November 1, 2018

On June 28, 2018, with subsequent minor amendments, the State of California enacted the California Consumer Privacy Act (CCPA), a law that generally restricts certain businesses' ability to collect and sell the "personal information" of consumers. While the law does not go into effect until 2020, the CCPA likely marks a major shift in the nation's data privacy regime. Even though the statute is to take effect in a single state, its broad jurisdictional reach would bring companies throughout the United States and from around the world into its sweep. Further, the CCPA is stepping into an area that is currently regulated in an often disjointed manner with both distinct and sometimes-overlapping federal and state provisions concerning data privacy. Acknowledging the potential significance of the new California law, Congress has recently held hearings to discuss some of these issues. This Sidebar begins by discussing the current legal framework governing data privacy, before briefly reviewing the CCPA's coverage and its provisions. While a few commentators have criticized the drafting and scope of the CCPA, this Sidebar does not focus on these issues, but instead evaluates how the law would function in its current form. The Sidebar then concludes by considering how the California statute is relevant for Congress, reviewing how various federal proposals could interact with the CCPA.

Current Legal Framework Governing Data Privacy. The present framework of data privacy regulation in the United States is best described as a "patchwork." No federal law exists that comprehensively regulates how entities across all industries collect and use consumer data. Instead, federal data privacy law involves a host of different laws covering various issues and sectors of the economy. For example, the Health Insurance Portability and Accountability Act (HIPAA) governs the privacy of individually identifiable health information, while the Children's Online Privacy Protection Act (COPPA) governs the protection of the privacy of children under the age of 13 in their interactions with online websites. And, to provide another example, the Gramm-Leach-Bliley Act (GLBA) regulates financial institutions, imposing

Congressional Research Service
7-5700
www.crs.gov
LSB10213

certain requirements aimed at safeguarding consumer data. Other sector-specific privacy statutes exist, but no federal statute purports to be a general sweeping regulation. Perhaps the broadest federal data privacy scheme is a product of the Federal Trade Commission's (FTC's) regulation of privacy through its authority to regulate "unfair or deceptive" acts or practices under the FTC Act of 1914. However, the FTC's authority is limited by the meaning of the phrase "unfair or deceptive," and at least one federal court has recently questioned the limits of that authority as it applies to digital privacy. One commentator has argued that this current federal framework for data privacy creates "overlapping and contradictory protections" that regulate only "certain sectors and types of sensitive information."

Adding to this federal mix are the laws of the 50 states. In addition to the CCPA, all 50 states have enacted statutes regulating how companies respond to "data breaches" involving personal information. In addition, most states have some sort of version of their own "unfair or deceptive" trade practice law, mirroring the FTC Act to various degrees, which, in turn, might apply to data privacy practices conducted by companies in those states. However, these laws offer varying levels of protection and may impact data privacy in different ways, if at all. With the passage of the CCPA, the quilt of federal and state data privacy laws appears to have become even more complex.

Who and What Does the CCPA Cover? The CCPA in the main applies to any "business" that collects the "personal information" of "consumers." "Consumer" is defined in the statute as a natural person who is a California resident. Other definitions warrant more explanation.

First, the statute's definition of "business" is fairly broad, and, unlike the federal patchwork provisions described above, the method of data collection or the industry that the business operates in does not limit the CCPA's reach. Instead, the CCPA applies to any company that collects the personal information of Californians, is for profit, does business in California, and satisfies one of three thresholds:

1. earns more than $25 million in annual gross revenues;
2. engages in the buying, selling, or receipt of the personal information of 50,000 or more California residents; or
3. derives more than 50% of its annual revenues from the sale of California residents' personal information.

Together, as several commentators have explained, these provisions will likely reach a considerable number of businesses with a website accessible in California, as businesses with even "relatively small" websites are likely to collect personal information (as defined below) from more than 50,000 Californians. Further, the "gross revenue" provision is not limited to revenue earned in the State of California, meaning that any business of sufficient size, regardless of where its revenue is earned, is subject to the CCPA if it collects the personal information of any Californians.

The CCPA does contain some narrow exemptions to its definition of "business." For example, the new California privacy law exempts businesses if "every aspect of [the] commercial conduct takes place wholly outside of California." The CCPA also exempts from its coverage the collection or sale of certain personal information if such activity is governed by federal statutes, including HIPAA, GLBA, and the Fair Credit Reporting Act. Lastly, the rights and obligations of the CCPA do not apply to the extent they infringe on the rights of other consumers, or the "noncommercial activities" of a person or entity "as described in" the free expression provision of the California Constitution.

Second, the CCPA's definition of "personal information" covers most information businesses collect from individuals. The law does not require the presence of any individual identifier, such as a name or address, for data to fall within the meaning of personal information. Rather, the CCPA broadly defines personal information as "information that identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Following this definition, the CCPA provides some telling illustrations of what constitutes personal information,

including any "electronic network activity [such as] browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement" and "inferences drawn from any of" this information.

The CCPA does exempt some categories of information from its definition of personal information. For example, personal information generally does not include "publicly available information," meaning information lawfully made available from government records. Similarly, the CCPA does not restrict a business's ability to collect "deidentified" or "aggregate consumer information," generally meaning information that cannot be linked in any way with particular consumers.

Notwithstanding these limitations, legal commentators have generally agreed that the CCPA's definition of personal information is "broad," capturing not just information that is expressly linked to a particular individual, but as well covering information that merely is "capable of being associated with" or "could reasonably be linked with" individuals or households. By contrast, the Children's Online Privacy Protection Act, mentioned above, defines "personal information" as "individually identifiable information about an individual collected online" such as a name, e-mail address, telephone number, or other specific identifier. The new California law's expansive definition of this term illustrates the intent of the CCPA's drafters about the statute's breadth.

What Will the CCPA Prohibit or Require? The CCPA provides consumers with three main "rights," the first of which provides consumers with the "**right to know**" the information that businesses have collected or sold about them. Under the new California law, businesses must, in advance of any collection, "inform [by mail or electronically] consumers as to the categories of personal information to be collected and the purposes" to which the information will be put. In addition to requiring this advance disclosure, under the CCPA a business must disclose, upon request, the specific pieces of personal information it has collected or sold from a consumer, the categories of sources from which the information was collected, and the third parties with whom the information was shared.

Second, the CCPA provides consumers the "**right to opt out**" of the sale of a consumer's information. Under the new law, businesses must inform consumers of this right, and if a consumer so affirmatively opts-out, the business cannot again sell the consumer's information unless the consumer subsequently provides the business express authorization. The CCPA contemplates future regulations from the California Attorney General allowing for the delegation of a consumer's authority to opt-out to another person.

Third, the CCPA gives consumers the right, in certain circumstances, to request a business delete any information collected about the consumer (i.e., "**right to delete")**. Under the law, a business that receives such a request must delete the information collected and direct its "service providers" to do the same. The CCPA provides for a few narrow exceptions to this right, including when the information is needed to complete a particular transaction for the consumer, to detect security incidents, or to "ensure the right of another consumer to exercise his or her free speech."

The CCPA's nondiscrimination rule backstops these rights. Specifically, the new California law provides that no business may discriminate against a consumer, including by "denying goods or services" or by "charging different prices or rates" to consumers who exercise their rights under the CCPA. However, the CCPA does permit businesses to "offer financial incentives" for the collection, sale, or non-deletion of personal information, and a business may offer a different price to consumers who exercise their rights "if that price…is directly related to the value provided to the consumer by the consumer's data." Nonetheless, the CCPA authorizes such financial incentives to be used only if the consumer provides the business "prior opt-in consent," which, in turn, may be revoked at any time.

Finally, the CCPA requires businesses to inform consumers about these rights in certain specific ways and provide the means to exercise them free-of-charge. For example, under the California law, businesses must provide in their privacy policy or on their website a description of a consumer's "right to know" and

"one or more designated methods" for submitting requests. The CCPA also requires businesses to educate their employees responsible for handling customer inquiries on the businesses' obligations and how to direct consumers in the exercise of their rights. Similarly, with respect to the "right to opt out," businesses must provide a "clear and conspicuous link" on their homepage entitled "Do Not Sell My Personal Information." The statute is unclear on how consumers must be informed of their right to delete, potentially raising the need for a future regulation or amendment to the statute to clarify the issue.

How will the CCPA be Enforced? The primary means to enforce the CCPA are enforcement actions brought by the California Attorney General. According to the statute, businesses that are in violation of the CCPA and do not cure those violations within 30 days are liable for civil penalties of up to $7,500 per violation. Penalties or settlements collected under the CCPA are to be deposited with the newly created "Consumer Privacy Fund," the funds for which are only used to offset costs incurred in connection with the administration of the CCPA.

While the CCPA provides for a private cause of action, this cause of action is only available in the case of a consumer whose "nonencrypted or nonredacted personal information" is subject to "unauthorized access and exfiltration, theft, or disclosure." Further, such actions can only be brought if a consumer provides a business with 30 days' written notice and provides the business with opportunity to cure the violation, unless the consumer suffered actual pecuniary damages. The statute does not specify how a business could "cure" a violation of this type. Consumers may recover damages under this section of no less than $100 and no more than $750 "per incident," or actual damages, whichever is greater, as well as injunctive relief.

The CCPA and Preemption. In the wake of the CCPA's passage, numerous commentators and industry representatives have called for a federal solution to fully preempt the CCPA. Other commentators, in favor of the CCPA's general approach, have argued that Congress should not displace the CCPA at all, or should only preempt it in the event Congress were to pass a "stronger" privacy law. Congress, assuming it were to pass a federal law seeking to displace the CCPA, would have many options in how to structure a preemption regime. As the Supreme Court recently explained in *Murphy v. NCAA*, there are three different types of preemption: "conflict," "express," and "field." And, as the *Murphy* Court observed, courts do not look for "a particular linguistic formulation when preempting state law." Rather, for Congress to preempt state law, it needs to enact a law that conflicts with the state law, expressly displaces the state law, or occupies the field of regulation "so comprehensively" that there is no room for supplementary state legislation.

If Congress were to adopt a comprehensive system for privacy, perhaps the most obvious means to preempt a broad swath of state regulation would be to do so explicitly within the text of the statute by including a specific preemption provision in the law. For example, several existing federal statutes expressly preempt all state law that "relate to" a particular subject matter. The Supreme Court has held that this language encompasses any state law with a "connection with, or reference to" the subject matter referenced. Similar language could be used to displace all state laws in the digital data privacy sphere. Similarly, with a comprehensive enough regime, a court could hold that Congress has regulated the entire field, crowding out state regulation by that means alone. As the Supreme Court stated in *Arizona v. United States*, "where Congress occupies an entire field, even complementary state regulation is impermissible." Further, as the Court has explained, federal law preempts state laws that pose an obstacle to the "accomplishment and execution of the full purposes and objectives of Congress." Congress could, by clarifying the purposes and objectives of a federal data privacy law in, for example, a findings section of a bill, attempt to implicitly preempt any state laws that run contrary to these goals. Nonetheless, the precise scope of obstacle preemption necessarily turns on a court's interpretation of a particular state law and a court's understanding of the purpose of the federal law.

As a more limited alternative, Congress could also elect to enact a federal data privacy framework that expressly preempts the CCPA and other state laws in certain ways, but not in others. For example, a

number of federal statutes preempt state laws that impose standards "different from" or "in addition to" the federal standards. The Supreme Court has generally held that such language does not displace state requirements parallel to or narrower than, the federal regulation. For instance, if Congress passes a statute that provides similar rights to the CCPA, it might displace only those aspects of the CCPA that provide for rights incompatible with the federal scheme. Any congressional law that declined to expressly preempt or create a conflict with aspects of the existing state schemes would thus leave the untouched state law elements in place. In order to ensure this result, Congress has in the past enacted so-called "savings clauses" or "anti-preemption provisions" that generally state that a federal statute does not override state law unless it is "inconsistent" with the federal statute. Congress could do the same with respect to federal data privacy legislation and, for example, state an intent to preempt some aspects of the CCPA, but not others. Ultimately, however, the preemptive scope of any federal data privacy legislation will turn on the "purpose of Congress" in enacting whatever law it chooses to enact and the specific language it uses to effectuate that purpose.