Legal Insights

Wolters Kluwer

October 17, 2019

What the Proposed CCPA Rules Mean for Business: The Good and The Bad

By Christian Auty and David Zetoony, Bryan Cave Leighton Paisner LLP*

The California Consumer Privacy Act ("CCPA"), which was enacted on June 21, 2018, has been the undisputed focal point of the data privacy world for the past year and a half. Its strange origins have become almost infamous. In early 2018 an activist appeared to be on the verge of passing, via referendum, what most argued at the time was a poorly drafted attempt to confer upon Californians certain rights in relation to the data that companies held about them, including the right of access (i.e., to find out what information a company holds) and the right to opt-out of the sale of information (i.e., to prevent a company from selling data about you). The California legislature stepped in at the last minute, and negotiated a legislative equivalent. The agreement was simple. The legislature would pass something like what the activist wanted, but, by using the traditional legislative mechanism, errors in drafting could be fixed at a later date via amendment, and fine-tune interpretation could be made through rulemakings that would come from the California Attorney General.

The expression goes that "Rome was not built in a day;" unfortunately the version of the CCPA that was enacted by the legislature basically was. From day one, and most likely owing to the speed with which the legislature put it together, it was riddled with drafting errors, confusing language, incorrect cross-references, and substantive edicts that made little business-practical sense. While nearly twenty amendments to the CCPA were proposed, only seven ultimately passed, with many problematic areas left unaddressed. The negative impact that the Act will have on business has been recognized by both the business community and the government. A consulting group hired by California's Office of the Attorney General to conduct an assessment of the impact of the CCPA on the economy of California estimated that the total cost of initial compliance with the Act would be $55 billion – i.e., 1.8% of California's entire Gross State Product.[1]

Within the business community many people hoped that the Attorney General would address head-on the areas of difficulty that remained.

---

* **Christian Auty** is Counsel with Bryan Cave and is an experienced advisor in the areas of data privacy, data breaches and distributed ledger technology. He advises clients on compliance with existing and anticipated data privacy regulations, including HIPAA and the GDPR, as well as state and federal regulations that pertain to blockchain technologies. **David Zetoony** is a partner with Bryan Cave and is an internationally recognized leader in the fields of data privacy and security. He has helped hundreds of companies navigate the complexities of privacy and security law from a business practical standpoint.

1 Berkeley Economic Advising and Research, LLC, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* at 11 (Aug. 2019).

On October 11, 2019, the Attorney General published a Notice of Proposed Rulemaking, and the text of Proposed Rules. While the Proposed Rules, if enacted, would marginally improve the ability of businesses to comply with the CCPA, they addressed few of the major business-community concerns that had been raised to the Office of the Attorney General which ranged from the interaction of the CCPA with AdTech, to the impact that CCPA on evidentiary privileges. Perhaps of greater concern, BCLP has identified over 40 areas of new business-community concerns raised by the Proposed Rules. In many ways the Proposed Rules are one step forward, three steps back.

Without parsing each of the areas in which the Proposed Regulations (if enacted) would improve the CCPA, or cause additional problems for business, the following outlines the top three improvements, and the top three areas of concern:

Improvements

1. Safe Harbor Mechanism for Authenticating a Consumer

The CCPA allows Californians to request that a company provide them "access" to the "specific pieces" of personal information that the company holds about them. The "right of access" is not a new concept. Health care companies and educational institutions have had to provide a similar access right for years under the Health Insurance Portability and Accountability Act ("HIPAA") and the Family and Educational Rights and Privacy Act ("FERPA"); in addition companies that are subject to the European General Data Protection Regulation ("GDPR") have also had to provide access to consumers when requested.

One of the risks that an access right creates is that a bad actor may be able to steal personal information about an individual by pretending that they are another person and then making an access request. Companies often feel as if they are between a rock and a hard place. If they make a consumer jump through too many hoops to prove their identity, they can get criticized for making it too difficult for people to exercise their right of access. Conversely, if they make it too easy to get access to information, a bad actor may abuse the system to steal information through fraudulent access requests potentially subjecting the respondent to liability.

The Proposed Rule provides certainty for business by stating that a company "may" take the following steps to authenticate an individual that submits an access request: (1) match three data points maintained by the business and, (2) request a "signed declaration under penalty of perjury that the requestor is the consumer."[2] While the Proposed Rule does not explicitly describe this authentication system as a "safe harbor," it would likely have that effect. The certainty that an approved authentication method provides is a positive for businesses that seek to comply with the CCPA.

---

2 NPR § 999.325(c). A slightly less onerous authentication method is also proposed for requests that would not result in "specific pieces" of information being conveyed. NPR § 999.325(b) (Verification for Non-Accountholders).

2. Fraud Detection

The CCPA implies that if a business transfers information to a third party "for consideration" and does not prohibit the third party from retaining, using, or disclosing the information, the transfer would be considered the "sale" of information. Once classified as a "sale," consumers would have, among other things, the right to "opt-out" and prevent such transfers.

The CCPA's definition of "sale" was extremely problematic for companies that pool information for the purposes of fraud detection or data security detection. Specifically, such companies often collect information from thousands of businesses across the country in order to flag suspicious individuals, IP addresses, or accounts. The information submitted by one business is often used for the benefit of others. Any "right" for an individual to opt-out of having their information shared in this type of network, could be misused by criminals to prevent companies from working together to flag fraud.

The Proposed Rule would clarify that if a business transfers information to a third party, and allows that third party to use, or disclose, the information to others, it is not a "sale." This provision, located in the Service Provider portion of the Proposed Rule, states that a service provider may use personal data provided to it for the benefit of other businesses "to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity" without losing service provider status. [3]

3. Disclosing Sensitive Information Through an Access Request

The CCPA of course allows Californians to request that a company provide them "access" to the "specific pieces" of personal information that the company holds about them. If a company that maintains your Social Security Number, Driver's License number, or financial account number, received an access request it would be required to disclose that information back to you. Forcing a company to disclose sensitive categories of personal information in response to an access request does little to help consumers (after all you already know your own Social Security Number), but does raise the possibility that bad actors will attempt to submit false access requests in order to extract valuable information that could be used for identity theft.

The Proposed Rules would allow a business not to disclose sensitive data fields (e.g., SSN, Driver's License Number, financial account number, or health insurance or medical information) in response to an access request.[4]

Areas of Concern for Businesses

1. Data Subject Request Statistics

Although the CCPA gives consumers the right to submit access, deletion, and opt-out-of-sale requests, it does not require businesses to publish how many requests they receive, or how they respond to those requests that are received.

---

3 NPR § 999.314(c) (Service Providers).

4 NPR § 999.313(c)(4) (Responding to Requests to Know and Requests to Delete).

The Proposed Rules would require that a business that "annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes" the personal information of 4 million Californians publish the number of requests received, complied with, or denied with respect to access, deletion, and opt-out. It must also publish the median number of days in which it substantively responded to such requests.[5] While the Proposed Rules do not contain an example of how this information would be conveyed, conceivably the Office of the Attorney General envisions something along the following lines added to company privacy notices:

	Total Received	Complied with in whole or in part	Denied
Access Requests			
Deletion Requests			
Opt-out of Sale Requests			
Median days responded			

Companies that are used to responding to data subject requests know that the amount of record keeping that would be required to comply with the Proposed Rule would be significant. Among other things, requests are often fluid, and change over time. As just one example, a consumer that submits an access request may later ask that it be deleted.

More importantly, it is not clear what utility such statistics would provide to consumers. Imagine if a company reports that they received 200 deletion requests, and denied, in whole or in part, 200. A 0% acceptance rate could be interpreted as suggesting that the company is failing to comport with the CCPA; it could also signify that the type of data held by the company is exempt from deletion requirements. (Indeed, it is unclear how such requests must be counted.) In a vacuum the statistic is meaningless. To the extent that it is used by privacy advocates (or eventually plaintiffs' attorneys) to conduct fishing expeditions into corporate privacy practices, it may be harmful.

2. Honor User Enabled Preference Settings

The Proposed Rule would require that a business treat user-enabled privacy controls, such as browser plugin or privacy settings, that communicate or signal a choice to opt-out of the sale of their personal information as a "valid request" to opt-out for that browser or device, or, if known, that consumer.[6] This requirement is, from a practical standpoint, unworkable.

As an initial matter, the Attorney General does not specify *what* "user-enabled privacy controls" would have to be honored. Would it be *every* plugin created for *every* browser, even if those plug-ins operated differently and conveyed different information? If so, how could companies possibly be aware of all new plug-ins and privacy controls that enter the market. Furthermore, many privacy settings and controls may be ambiguous as to whether the consumer is attempting to opt-out

5 NPR § 999.317(g)(1)-(3) (Training; Record Keeping).
6 NPR § 999.315(c) (Requests to Opt-Out).

of the sale of information. Take, for example, the "Do Not Track" header. If a consumer enabled the header in their browser, would that signal for a company that it cannot *sell* information? That it cannot *track* the consumer? That it cannot *sell* information about the consumer that could be used for tracking by others?

3. Authorized Agents

The Proposed Rule states that a consumer could make a request for access or deletion through an "authorized agent." If an authorized agent approaches a business, the business could require "written permission" that shows the agent is empowered to act on behalf of the consumer.[7]

At first glance this seems like a reasonable proposal. A consumer could ask someone else to seek information on their behalf, and a company can ask for proof that the agent is empowered to act. The Proposed Rule does not, however, discuss how the proposal would interact with the eSign Act – a federal statute that effectively states that electronically signed documents should be considered on par with paper documents. Nor does the Proposed Rule acknowledge or discuss the practice that has emerged in Europe of third parties establishing Apps that enable consumers (or individuals posing as a consumer) to blast out hundreds or thousands of data subject access requests in a couple of minutes – often times going to businesses that the consumer has never interacted with. The reference to "authorized agents" in the Proposed Rule opens the door to permitting the development of similar apps in the United States that would exponentially increase the number of spurious access and deletion requests, raise questions about how much proof a company is allowed to demand that such requests are, in fact, coming from specific consumers, and would clog the privacy departments of most companies as they attempt to deal with spurious request.

7 NPR § 999.326(a)(1) (Authorized Agent).