

## insights

TYPES NOT MAPPED YET October 14, 2019 | TTR not mapped yet | Luke Sosnicki

# What businesses need to know about the Attorney General's proposed CCPA regulations

On October 10, 2019, California's Attorney General released its long-awaited draft regulations explaining how the state intends to enforce the requirements of the California Consumer Privacy Act (CCPA). While there are a handful of bright lines - or as close to bright lines as such a broad statute could permit - the regulations leave much more to the best judgment of businesses that will be doing their best to comply.

Many of the more bright-line provisions are in direct response to questions that the public and industry raised during the informal comment-gathering process that began earlier this year. Examples include:

### **"Do Not Sell My Info" button or logo**

The draft regulations do not currently include a template for a "Do Not Sell My Info" button. But they do include a space for such a button, which will be made available for public comment, and will presumably be made a part of the final regulations. Notably, while a template for a button will likely be a part of the final regulations, businesses will still need to develop their own forms that explain to consumers their right to opt out.

### **Timing of responses**

The regulations clarify that the 45-day period to respond to verifiable consumer requests (VCRs) starts from the date the company receives the request, not from the date the company is able to verify the consumer's identity. Businesses must acknowledge receipt of VCRs in 10 days, and must act on consumers' requests to opt out of the sale of their personal information as soon as "feasibly possible," but no later than within 15 days.

### **Service providers**

The regulations clarify a few important points for service providers. A service provider is an entity that "processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract." A company's disclosure of consumer information to a service provider is not a "sale," and therefore does not fall within a consumer's right to opt out of the "sale" of personal information. It is also important to note that those falling within the definition of a service provider under CCPA are not deemed a "third party."

The regulations first clarify that service providers working for entities that are not "businesses" under the CCPA (for example, non-profits) will still be treated as service providers. This clarification was necessary to ensure that non-profit entities that use for-profit service providers are not unwittingly brought back within the statute's scope. The regulations next clarify that service providers authorized by a business to collect information directly from consumers can still be service providers. This was necessary to clarify that service providers will not necessarily lose that designation if they interact directly with consumers and do not receive all of their consumer information solely from a covered business.

Finally, the regulations provide that a company may be a service provider with respect to consumer information received from a business pursuant to a contract, but may also be a covered business itself with respect to information that the company collected outside of any such contract.

### **Recordkeeping**

The regulations add recordkeeping requirements that the statute itself does not impose. Businesses must keep records of their CCPA compliance for at least two years. To address the problem of the recordkeeping requirement itself creating a data-security risk, the information may be kept in a log format that includes only such information

as the date and nature of the request, the nature of the response, and the time it took the business to comply. The regulations also require companies that process more than 4,000,000 records to disclose certain CCPA-compliance metrics in their privacy policies, as well as to establish CCPA training policies for employees.

This, for better or for worse, is where most bright lines end. The Attorney General's draft regulations addressing what information businesses must include in their responses to consumer requests, how companies are to verify consumers' identities, and when companies are supposed to decline deletion requests all require businesses to figure out what is "reasonable" under the circumstances. The Attorney General's Office explained that this was by design, expressly noting in its published Initial Statement of Reasons (ISOR) that the regulations were intended to give businesses a good amount of "discretion" and "flexibility" in implementing the CCPA.

### **"Risk-based" approach to responding to consumer requests**

In addressing what information businesses must disclose in response to a consumer request, the regulations discuss a "risk-based" approach that "balanc[es] a consumer's right to know about their personal information collected, used, and shared by a business with the consumer's interest in preventing the disclosure of their personal information to unauthorized persons." Under this approach, businesses are categorically prohibited from disclosing Social Security numbers, driver's license numbers, financial account numbers, any health or medical information, passwords, or security questions and answers in response to consumer requests. As to other specific pieces of information, however, businesses must themselves determine whether disclosure "creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks." If so, the information must not be disclosed.

### **"Reasonable" method of verification**

The regulations require businesses to establish and comply with "a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information." The regulations then list six different factors for businesses to consider in deciding what is "reasonable," including such things as the "type, sensitivity, and value of the personal information," the risk of harm to the consumer from unauthorized access, the manner in which the business interacts with the consumer, and the technology available for verification. Businesses are further directed to establish "reasonable security measures" to detect fraudulent identity-verification activity.

While the term "reasonable" is not specifically defined (as it rarely is in the law), the regulations do provide some helpful guidance as to verification by listing baseline practices that the Attorney General expects. For consumers who already maintain password-protected accounts with the business, a business may use its existing authentication practices to comply with the CCPA's verification requirements. For consumers who do not maintain such accounts, the regulations set up a two-tier system. This system requires two-data-point matching for consumer requests to know categories of personal information, and three-data-point matching plus a sworn declaration from the consumer for requests to know specific pieces of information. A business complying with such a request must keep a copy of the declaration as part of its recordkeeping responsibilities.

### **Discretion to deny deletion requests**

The regulations state that businesses "may" refuse to delete information if they cannot verify the requesting consumer's identity. The word "may" (as opposed to "shall") is intentional. In its ISOR, the Attorney General's office noted that using the word "may" gives businesses discretion whether to honor the request anyway. Notably, the regulations are entirely silent on how companies may interpret and apply the nine different categories of information that businesses may keep despite a deletion request. These include such broad (and undefined) categories as information necessary to complete a transaction that the consumer requested, to detect fraud, to exercise free speech rights, to comply with a legal obligation, and to use the information "internally ... in a lawful manner that is compatible with the context in which the consumer provided the information." Deciding how to interpret and apply these categories entails a good amount of discretion as well.

### **Valuing personal information**

The value of a consumer's data to the company is another important determination the regulations require businesses to make. Under the CCPA's non-discrimination provision, a company that provides a financial incentive based on whether the customer has exercised an opt-out right may only do so if the incentive is "reasonably related to the value of the consumer's data to the business." The regulations further require the business to explain that calculation to consumers. The problem, as the Attorney General's office readily concedes, is that there is no standardized methodology for valuing consumer data. Recognizing this, the regulations permit eight different ways for businesses to come up with this number, including a catch-all category of "any other practical and reliable method of calculation used in good faith." Yet again, the terms "practical" and "reliable" are left for businesses to decipher.

### **Notices**

The regulations devote a significant amount of their space to required notices to consumers, specifically:

1. Notice at collection of personal information

2. Notice of right to opt-out of the sale of personal information

3. Notice of financial incentives

4. The business' privacy policy

While the regulations provide guidance on the information that must be included in each type of notice, the regulations do not discuss the interaction of the different notices or whether required notices may be grouped together.

#### **Business purpose**

Another point lacking clarity under the statutory language of CCPA is in the definition of "business purpose," a term used in several contexts in the law. Section 140(d) provides a definition on the types of uses of personal information covered by the term, then includes seven specific business purposes. In using the language "[b]usiness purposes are:" before listing the seven items, the statute does not make clear whether the seven items are illustrations of business purposes or constitute the full list of permissible business purposes. While the regulations do not directly address the point, in a footnote in the ISOR the Attorney General's Office cites to the definition of business purpose without the seven items. This would appear to militate toward the interpretation of the seven items as illustrative rather than exhaustive.

The regulations do not provide additional guidance regarding the scope of exemptions to CCPA, including the exemption for personal information subject to the requirements of the federal Gramm-Leach-Bliley Act or the California Financial Information Privacy Act. This exemption has been the subject of significant discussion among financial institutions.

The regulations' heavy reliance on "reasonableness," along with the Attorney General's intentional allowance of wide "discretion" and "flexibility" for businesses in implementing the CCPA, certainly portends some very interesting enforcement activity next year. We will be analyzing specific provisions in more detail in future blog posts, so please be sure to check back.

The deadline for initial comments is December 6, 2019.

#### **authorsTest**

A dark grey rectangular profile card with a blue horizontal bar at the top. It contains the name 'luke' in white lowercase letters and 'Luke Sosnicki' in smaller white uppercase letters below it.

**luke**

Luke Sosnicki