CEP Magazine - February 2020

The draft CCPA regulations reviewed: Key takeaways

Jana Terry, JD, CCEP-US, CIPP/US, CFE

Jana Terry (jterry@becksteadterry.com) is a partner with Beckstead Terry PLLC, a boutique employment, compliance, and privacy law firm in Austin, Texas, USA.

- Becksteadterry.com/our-team/
- linkedin.com/in/jana-terry

On October 10, 2019, the California Attorney General's office published draft regulations to operationalize the California Consumer Privacy Act (CCPA).[1] Although the draft regulations are still subject to comment and will not be in final, enforceable form until July 2020, they provide helpful insights into how the final regulations are likely to look. And they are the only guidance that companies have as they start to implement the now-effective CCPA. These are the key takeaways from the draft regulations that companies should consider as their CCPA compliance programs go into effect.

Expect initial compliance costs to be high

In conjunction with the draft regulations, the California Department of Justice published an Economic Impact Statement that recognizes that the CCPA will have a large impact.[2] The attorney general projects that it will initially cost the "typical" business $75,000 to come into compliance with the CCPA. Annual ongoing costs (for "typical" businesses) are predicted to be $2,500 per year. For small businesses, the initial costs are predicted to be $25,000, and the ongoing costs are predicted to be $1,500 per year. These numbers are an indication of how seriously businesses are expected to take their obligations. For compliance professionals who are having trouble obtaining adequate resources to implement effective CCPA compliance programs, citation to the attorney general's expectations may be helpful to their arguments.

How to comply with notice obligations: Consult the regulations

The draft regulations are substantially easier to understand than the text of the CCPA, particularly with respect to the who, what, when, where, and how of providing notices to consumers. The draft regulations break down the notice obligations into four types: (a) Notice at Collection of Personal Information (PI), (b) Notice of Right to Opt-Out of Sale of PI, (c) Notice of Financial Incentive, and (d) Notice of Consumer Rights (via the Business's Privacy Policy).[3] All of these notices must be

easy to read, understandable to the average consumer, posted conspicuously and in an attention-getting format, accessible to consumers with disabilities, and available in the languages in which the business provides other information to consumers. The contents of the notices are specified by the draft regulations.

Notice at collection

This is the notice that must be provided to consumers at the point where PI is going to be collected. It must contain the following information (or a link to the section of the business's privacy policy that contains the same information):

- A list of categories of PI that is collected about consumers;
- For each of the categories, the business or commercial purpose for which the information will be used;
- If the business sells PI, a link titled either "Do Not Sell My Personal Information" or "Do Not Sell My Info." (In the case of offline notices, provide the web address for the webpage to which the "Do Not Sell" link directs consumers); and
- A link to the business's privacy policy. (In the case of offline notices, provide the web address of the business's privacy policy).

Notice of right to opt-out of sale of PI

A business that "sells" PI (as defined in the CCPA) must post the notice of right to opt out on the web page to which the consumer is directed after clicking the "Do Not Sell" link on the download or landing page of a mobile application. It must contain the following information (or a link to the section of the business's privacy policy that contains the same information):

- A description of the opt-out right;
- The web form by which the consumer can submit their request to opt out online or, if the business does not operate a website, the offline method by which the consumer can submit an opt-out request;
- Instructions for any other method by which to request to opt out;
- Any proof required when a consumer uses an authorized agent to exercise the opt-out right—or, in the case of a printed form containing the notice, a web page, online location, or URL where consumers can get information about authorized agents (the possibility of consumers exercising rights through an authorized agent is mentioned several times in the draft regulations; companies need to anticipate that this may be common); and
- A link to the privacy policy (or, if offline, the URL of the web page where consumers can access the privacy policy).

Notice of financial incentive

If the business offers a financial incentive or price or service difference (a "financial incentive") in connection with obtaining PI, the business must post a notice with the following information:

- A "succinct" summary of the financial incentive;
- A description of the material terms, including the categories of PI that are implicated;
- How the consumer can opt in;
- The consumer's right to withdraw at any time and how to exercise that right; and
- An explanation of why the financial incentive is permitted under the CCPA, including a good faith estimate of the value of the consumer's data and how that value was calculated.

Privacy policy

According to the draft regulations, the purpose of the privacy policy is "to provide the consumer with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information." In addition to the easy-to-read and accessible requirements for all CCPA-required notices, the privacy policy must:

- Be available in an additional format that a consumer can print out as a separate document, and
- Be posted online through a conspicuous link using the word "privacy" on the business's website homepage or on the download or landing page of a mobile application. (If the business does not operate a website, it must make the privacy policy conspicuously available to consumers).

With regard to content, the draft regulations provide a detailed explanation regarding how the privacy policy must:

- Advise consumers about their CCPA rights;
- Provide instructions about how consumers can exercise their rights and describe the verification process;
- List the categories of PI the business has collected in the preceding 12 months and, for each category, provide:
    - The business or commercial purpose for collecting the PI.
    - The "categories of third parties" with whom the PI is shared. According to the draft regulations, categories of third parties means "types of entities that do not collect personal information directly from consumers including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers."
- State whether or not the business sells the PI of minors under 16 years old without affirmative authorization;
- State whether the business has disclosed or sold any PI to third parties for a business or commercial purpose in the preceding 12 months and, if PI has been sold or disclosed, list the categories of PI disclosed or sold;

- Explain how a consumer can designate an authorized agent to make CCPA requests on the consumer's behalf;
- Provide a contact for questions or concerns using a method that reflects the manner in which the business primarily interacts with consumers;
- Identify the date the privacy policy was last updated; and
- If the business annually buys, receives, sells, or shares the PI of 4 million or more consumers, disclose certain metrics regarding the number of CCPA requests and the median number of days that it took the business to respond.

For businesses' data practices, transparency will be difficult to avoid

In general, the draft regulations reflect an effort to encourage businesses to be more transparent about their data practices and make it easy for consumers to exercise their CCPA rights. In several instances, the draft regulations close what might otherwise be "loopholes" for businesses. A consumer request that is close but not quite technically correct under the statute will be "deemed" to count as a proper request to which businesses are obligated to respond. In other words, "close" counts in horseshoes and the CCPA, but only if you are a consumer.

For example, businesses cannot ignore right-to-know or delete requests that are submitted in a manner that is not one of the methods designated by the business, or are deficient in some respect unrelated to the verification process. Instead, the business *must* either (a) treat the request as if it had been submitted by the designated manner or (b) provide the consumer with specific directions on how to submit the request or remedy any deficiencies.[4]

In some cases, a business is not permitted to require the consumer to resubmit the request or correct deficiencies before the business is obligated to provide a substantive response. Instead, the consumer's technically deficient request is "close enough" to be "deemed" to count as a different request. Here are three examples:

1. If a business denies a consumer's request to delete personal information because the consumer's identity cannot be adequately verified, the request for deletion is "deemed" to be an exercise of the right to opt out of the sale of PI.[5] In other words, the denial of a request for deletion (on verification grounds) must be treated as if the consumer had clicked on the "Do Not Sell My Personal Information" link.
2. If a business cannot verify a consumer's request for *specific pieces* of PI, the business must treat the request as if it were, instead, a request for *categories* of PI.[6]
3. Businesses that collect PI online must treat user-enabled privacy controls, such as a browser login or privacy setting or other mechanism, as if they were statutory requests to opt out.[7] This is a significant new compliance obligation that will be technologically challenging. Whatever system is put in place to receive and respond to opt-out requests will have to be technologically capable of recognizing, at the point where a consumer is entering PI, privacy settings of all sorts and processing them as opt-out requests (which can be reversed only by a

confirmed affirmative choice to opt back in, not a simple change in the privacy settings during a subsequent visit to the website). If the CCPA did already adequately incentivize businesses to stop selling data, the complexity of this regulation may do the trick.

Finally, the draft regulations require businesses to maintain records of all CCPA consumer requests and how the business responded to those requests. Businesses may use a ticket or log format so long as the documentation includes the date, nature, and manner of the request; the date and nature of the business's response; and the basis for any denial (in whole or in part). This information must be maintained for 24 months, and this retention will not cause the business to violate the CCPA.[8]

Don't forget about data security

Compliance with the CCPA disclosure requirements will result in two new points of data breach vulnerability: disclosure of PI (because PI may be inadvertently disclosed to the wrong person) and transmission of the PI (if the transmission method is not adequately secure). Although the draft regulations favor transparency about *business data practices*, the same is not true for *consumer PI*. In short, the proposed regulations "balance the consumer's right to know with the harm that can result from the inappropriate disclosure of information" and attempt to "reduce the risk that a business will violate another privacy law."[9]

The attorney general emphasizes that verification of the consumer's identity before providing PI in response to a request is critical. Any missteps at this point in the process can result in data breaches.

The draft regulations require businesses to establish, document, and comply with a "reasonable method" for verifying the requesting consumer's identity. When determining verification methods, businesses should follow the guiding principles outlined in the draft regulations and should consider certain identified factors. One guiding principle is that businesses should verify consumer identity either by matching information provided by the consumer to information that the business already possesses or by using a third-party verification service. Businesses should *not* collect additional PI in order to verify identity unless it is necessary to do so, in which case the additional PI should be deleted as soon as possible.

The draft regulations provide guidance, examples, and a "baseline" of what would constitute a reasonable method for verifying consumer identity before responding to requests to know and to delete, depending upon whether the consumer holds a password-protected account with the business. Additionally, the draft regulations require a two-step process before processing certain requests. Regardless of what method businesses choose to use for verification, the draft regulations require that the business also implements "reasonable security measures" to detect fraudulent identity verification activity. Additionally, when transmitting PI in response to a verified request, the business must employ "reasonable security measures."

Finally, in some cases, the attorney general has determined that the risks are simply too high to permit disclosure, no matter what the CCPA says. Specifically, the draft regulations *prohibit*—regardless of verification and no matter what method is used—disclosure of any of the following: Social Security numbers, driver's license numbers or other government-issued identification numbers, financial account numbers, health insurance or medical identification numbers, account passwords, or security questions and answers (the "Highly Sensitive PI"). Businesses will need to be vigilant about this. When a consumer requests specific pieces of information, the Highly Sensitive PI will have to be redacted.

Table 1 outlines the verification guidelines[10] and business response requirements and options[11] per the draft regulations.

Requests to opt out	
Verification Procedures	Business Response Options/Requirements
No verification required	**Deadline:** Must act on an opt-out request within 15 days **90-day lookback:** In addition to stopping any future sales of PI, the business must notify all third parties it has sold PI to in the preceding 90 days and instruct them not to further sell information. The business must inform the consumer when this is completed.
Request for categories of PI	
Verification procedures	Business response options/requirements

Password-protected accounts: The business can use its existing authentication practices. However, businesses should not disclose or delete data until consumers have re-authenticated themselves. **No password-protected account**: The business cannot comply with the request unless it can verify the identity of the consumer to a "reasonable degree of certainty." This may include matching at least two data points.	**Preliminary response**: Within 10 days from receipt of the request, the business must provide a preliminary response in which it acknowledges receipt of the request and describes its procedures for verifying and handling the request. **Substantive response**: The business will have 45 days to provide a substantive process. This 45-day period includes the verification process; it can be extended by another 45 days for a maximum of 90 days total. **If the requestor is verified**, the business must use reasonable security methods to transmit the following individualized response: • The categories of PI collected about that consumer, • The categories of sources of PI for each of those categories, • The purpose of collecting that PI, • The categories of third parties to whom the PI is sold or disclosed, and • The business or commercial purpose for the sale/disclosure. The business should not respond by reference to the notice at collection or the privacy policy unless the response would be the same for all consumers and the policy contains all of the required information. **If the business cannot verify the identity of the requestor**, the business **may** deny the request. If the request is denied in whole or in part, the business must inform the requestor that it cannot verify their identify and provide or direct the consumer to its general data handling practices as set forth in the privacy policy.
Requests for specific pieces of information	
Verification procedures	**Business response options/requirements**

Password-protected accounts: Same as requests for categories of PI **No password-protected account**: The business cannot comply with the request unless it can verify the identity of the consumer to a "reasonably high degree of certainty." This is a higher standard and would require, for example, matching three data points *plus* obtaining a declaration, signed under penalty of perjury, that the requestor is the consumer whose PI is the subject of the request. Such signed declarations must be retained by the business as part of their record-keeping obligations.	**Preliminary/substantive response deadlines:** Same as requests for categories of PI **If the requestor is verified**, the businesses should transmit the specific pieces of information using "reasonable security measures." If the consumer has a password-protected account, that account can be used if it meets the requirements. However, the Highly Sensitive PI must **never** be disclosed and must be redacted from any specific pieces of PI that are provided before the disclosure is made. Businesses are also prohibited from providing consumers with specific pieces of PI "if the disclosure creates a substantial, articulable and unreasonable risk to the security" of that PI, the consumer's account with the business, or the security of the business's systems or networks. **If the requestor cannot be verified**, the business **must** deny the request, inform the consumer that it cannot verify their identity, and process the request as if it were a request for categories of PI collected about the consumer.
Requests for deletion	
Verification procedures	**Business response options/requirements**

Business discretion: The business must determine the verification standard based on the sensitivity of the PI and the risk of harm to the consumer posed by unauthorized deletion. For example, deletion of family photographs and documents may require a reasonably high degree of certainty, but deletion of browsing history will require only a reasonable degree of certainty.
 	
In addition to the verification procedures that a business should establish, the choice to delete (if exercised online) must be confirmed through a 2-step process.
	Preliminary/substantive response deadlines:
	
	Same as requests for categories of PI
	
	If the request is verified (and confirmed through a two-step process, if applicable) and the business grants the request, the business must:
	• Delete by permanently and completely erasing the PI on its existing systems and backup systems, de-identifying the PI, or aggregating the PI. (With regard to backup systems, the draft regulations permit businesses to delay the deletion until the next time that they access the backup system.)
	• Respond to the consumer by disclosing:
	  ◦ How the PI was deleted, and
	  ◦ That the record of the request and business response will be maintained.
	
	If the verified and confirmed request is in any respect denied, the business must:
	• Tell the consumer that it is denying the request and explain the reason (including any applicable statutory or regulatory exception),
	• Delete any PI that is not subject to the exception, and
	• Not use any PI retained for any purpose other than provided for by the applicable exception.
	
	If the requestor cannot be verified, the business may deny the request. If the business denies the request, it must inform the requestor of the decision and process the request for deletion as a request for opt out.

Table 1: CCPA verification guidelines

Make sure consumers have more than one way to exercise their rights

The draft regulations contain a number of clarifications and obligation enhancements. In addition to those highlighted above, the proposed regulations contain other requirements that go beyond the CCPA text. For example, under the CCPA, a business is required to designate at least two methods for consumers to exercise their CCPA rights. One method must be a toll-free number. If the business has a website, the second method must be via the website. However, the draft regulations go further and

provide that one of the designated methods must reflect the manner in which the business primarily interacts with the consumer. If the manner in which the business primarily interacts with the consumer is neither online nor by phone, then the business will be required to designate another method—in addition to the website and toll-free number—even if that raises the requirement to *three* methods.[12]

Second, whereas the CCPA requires businesses to provide training only on certain sections of the CCPA, the draft regulations provide that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA must be trained on *all* requirements of the CCPA. Additionally, they must be informed of the regulations and how to direct consumers to exercise their rights under the CCPA and the regulations.[13]

The draft regulations also provide more guidance and clarifications regarding service providers, special rules regarding minors, how companies offering financial incentives for the collection of PI can determine the "value" of the data, and how businesses that do not collect PI directly from consumers should handle data requests. If these issues are of concern to your business, you should read the applicable sections of the draft regulations so that you have a preview of how the final regulations may take shape.[14]

Takeaways

- Be prepared for initial compliance costs to be high.
- The draft regulations provide helpful specifics on how to comply with notice obligations.
- The draft regulations indicate that it is going to be hard for businesses to avoid transparency about their data practices.
- In your effort to comply with CCPA disclosure requirements, don't forget about data security.
- You may need to provide more thorough training and/or designate an additional method for consumers to exercise privacy rights.

1 California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 to 1798.198 (West 2018).
2 California DOJ, "STD 399 - Economic and Fiscal Impact Statement," August 14, 2019, http://bit.ly/34f4Qzn.
3 California DOJ, "California Consumer Privacy Act Regulations: Proposed Text of Regulations" (to be codified at 11 CCR §§ 999.300-999.341), http://bit.ly/34obZgQ.
4 11 CCR § 999.312(f).
5 11 CCR § 999.313(d)(1).
6 11 CCR § 999.313(c)(1).
7 11 CCR § 999.315(a).
8 11 CCR § 999.317(c)-(d).
9 California DOJ, *Initial Statement of Reasons,* § IV.H, http://bit.ly/2pNXdRq.
10 11 CCR § 999.323-325.
11 11 CCR §§ 999.312, 999.313, and 999.315.
12 11 CCR § 999.312(c).
13 11 CCR § 999.317(a).

14. 11 CCR §§ 999.314, 999.330-332, 999.336-337, and 999.305(d).