THE
NATIONAL LAW REVIEW

California Consumer Privacy Act: Are You Ready? (Part 2)

Article By
Susan Kohn Ross
Mitchell Silberberg & Knupp LLP

- Communications, Media & Internet
- Consumer Protection

- California

Tuesday, October 22, 2019

In **Part 1**, we summarized the recent legislative changes regarding the California Consumer Privacy Act ("CCPA"). Bearing in mind the CCPA takes effect on January 1, 2020 and the Attorney General is required to issue regulations by July 1, 2020, these regulations both meet that time frame, but also seek to provide much-needed guidance to industry.

Most of the legislative changes focused on narrowing the definition of personal information, clarified the time frame which applies when a consumer demands information the business possesses about him or her, and also confirmed the CCPA applies to businesses, not non-profits or government entities. In this Alert, we summarize the regulations which were recently issued. However, even in the regulatory context, the starting point remains the same. Companies should begin by asking the following questions:

1. Is our annual gross revenue at least $25 million (not limited to California income alone)?

2. Do we have the personal information of at least 50,000 California consumers, households or devices?

3. Do we sell* the personal data we have of those California consumers, households or devices? If so, do we derive 50% or more of our annual revenues from those sales?

4. Even if we do not sell that personal data, do we disclose* any portion of it to any third parties?

* Definitions for both “sell” and “disclose” appear below.

The term “consumer” has been defined from the outset as anyone who lives in California. Devices are defined at Civil Code § 1798.140(j) as “any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.”

The regulations finally provide a definition for household at proposed Civil Code § 999.301(h) to mean “a person or group of people occupying a single dwelling.” The term “privacy policy” is also expanded at proposed Civil Code § 999.301(m) to mean a statement the business provides describing its practices on and off line regarding the “collection, use, disclosure and sale of personal information and of the rights of consumers regarding their own personal information.”

For regulatory purposes, the following questions should be added to the list:

1. Does our website serve all our users or do we have a California only facing section of our website?

2. Do we have a privacy policy on our website? If so, it is conspicuously displayed?

3. Do we currently track when users accept our terms and conditions**?

4. Do we keep a record of the changes we make to our terms and conditions** each time we update?

5. Is the means we use to receive acceptance of our privacy policy by users adequate to meet our current and future needs?

** While we are focused on the privacy policy for CCPA compliance purposes, the same general concept of tracking acceptances for terms of use applies. Do you retain versions that are updated and replaced? Do you apply version numbers or dates to track changes? Do you track acceptance by users when new versions are posted? If so, how long do you retain those records? Do you rely on click-through acceptance or other means? Do you notify users by email when terms and conditions are updated?

The reason for these questions will become apparent as we discuss the new regulations. See here for the full regulatory details. The starting point is these regulations were issued as a proposal. The deadline to comment is 5:00 p.m. on December 6, 2019 (to PrivacyRegulations@doj.ca.gov or Privacy Regulations Coordinator, California Office of the Attorney General, 300 S. Spring St., First Floor, Los Angeles, CA 90013). Public hearings will also be held on December 2 (Sacramento), December 3 (Los Angeles), December 4 (San Francisco), and December 5 (Fresno).

The regulations focus on permitting consumers to obtain the basic information called for in the CCPA:

1. What specific pieces of personal information the business collected;
2. The categories of personal information collected and sold about that consumer;
3. The purpose for which the personal information was collected or sold; and
4. The categories of third parties to whom the business sold or disclosed that data.

The business must provide two or more means by which the consumer may submit a request for information, one must be a toll-free phone number and, if the business has it, a website (if no website, the business must find other acceptable means of giving notice). The information must be provided within 45 days (an additional 45 days is possible for good cause, but does not extend the time within which the first response must be given). The data must be provided free of charge, the business may impose reasonable means to verify the identity of the recipient, and, when providing the data, it must be in an easily transferrable format. If the company declines to act on the request, such as because it cannot verify the requestor, it must still respond within the first 45 days, and explain the applicable appeal rights. The response process is discussed again below where more specifics are provided.

When it comes to verification, as noted, the method must be reasonable. The regulations define reasonable to include a consideration as to the sensitivity of the information and the risk of harm to the consumer from unauthorized access or deletion. If the consumer has a password protected account, that account may be used to provide the notice and also to detect any fraud. When it comes to non-account holders, at least two data points must be matched, and the result must yield a high degree of certainty. In some cases, a third data element can be required along with a signed declaration under penalty of perjury. When it comes to deletions, companies would be well advised to consider whether to rely on the password protected account, or more data points, depending again on the sensitivity of the data and the risk of harm to the consumer by unauthorized deletion.

The consumer data disclosed is for the 12 months preceding the date of receipt. Consumers may not make more than two (2) such requests in any 12 month period. The business may charge the consumer only if the requests are unfounded or excessive. If the consumer requests deletion of his or her records, that request is also subject to the 45 day rule. However, there are some exceptions. Companies may retain the data in order to:

1. Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, perform actions reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
2. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity.
3. Debug to identify and repair errors that impair existing intended functionality.

4. Exercise free speech, ensure another consumer's right to exercise free speech, or exercise another right provided for by law.

5. Comply with the California Electronic Communications Privacy Act.

6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

7. Enable solely internal uses reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

8. Comply with a legal obligation.

9. Use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

It is reasonable to anticipate that those businesses whose function is not platform related are most likely going to primarily rely on (1) completing the intended transaction, (7) use the data as expected, and (9) use the information in a lawful manner (see points above). This means companies must be careful how they describe why they are collecting the data and what they intend to do with it. This means, for example, that if one of the routine actions your company takes with consumer data is to distribute marketing materials, your privacy policy will now need to specifically mention that use. The Privacy Policy itself must also be posted online through a conspicuous link using the word "Privacy" which must be positioned on the home page of the website or the landing page of the mobile app.

The CCPA also includes the right to opt-out, which is why determining in advance what exactly is done with the data collected is critical. If you share that data with any third parties, you are obligated to provide an opt-out option. That is the case because the definition of "selling" includes "selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or third party for monetary or other valuable consideration". See Civil Code § 1798.140(t).

The rules about minors are unchanged. For minors under the agent of 13, the consent of a guardian or parent is required for all purposes, including consent to sell. If the minor is between 13 and 16, the minor must give consent for all purposes.

Businesses may not discriminate against consumers who exercise their CCPA rights. Discrimination is broadly described to include denying goods or services, charging different prices or rates, or providing a different level of service or quality of goods. However, such differences are permitted, including financial incentives, if that difference is reasonably related to the value provided to the business by the consumer's data. More on this topic can also be found later.

There are specific disclosures also required:

1. At or before the point of collection, the business must inform the consumer as to the categories of personal information collected and the purposes for which that data is collected. If the business later decides it wants more data or it wants to put the existing data to different uses, it must first obtain the consumer's consent.

2. The method and means by which the consumer may opt-out. This includes the need to have a "clear and conspicuous" link on the website titled "Do Not Sell My Personal Information" or "Do Not Sell My Info." The Attorney General intends to provide a recommended logo format, but wants input before finalizing the design. This notice is to appear on the home page of the website or the landing page of the mobile app.

3. Any financial incentives which are offered must be stated.

4. The privacy policy must also include a description of the consumer's rights under the CCPA, how he or she may submit requests for disclosure, deletion and opting-out, and, of course, additional information about data collection and sharing practices. This would seem to mean the same data would appear in two places – once at sign-up and once in the Privacy Policy itself. However, elsewhere, there is an indication notice may be provided through a link to the relevant section of the online privacy policy.

5. Training is also required of the individuals responsible for handling consumer requests, to include directing consumers to how they may exercise their CCPA rights. The Attorney General has interpreted this provision to apply only once the business handles 4 million or more consumer records. Such entities will also be required to post online the number of requests to know, delete and opt-out received in the previous calendar year, and the median number of days in which they took to respond.

Other recommendations from the Attorney General include being sure to use "plain, straightforward language, a format that draws the consumers' attention to the notice, and providing the notice in the languages in which the business providers consumer contracts, and other things" which mirrors the requirements of proposed Civil Code § 999.305(a)(2). Those requirements include access for those with disabilities. The regulations underscore that notice must be given prior to the collection of any information, but the notice itself may be given by providing a link to the relevant section of the online privacy policy.

If the business receives the data strictly from other sources, it need not give notice of collection to the consumer but must either contact the consumer directly and provide that notice or contact the source of the information and confirm the source has provided the required notice and obtain a signed attestation from that source describing how the source gave notice, to include a copy of the notice. These attestations are to be retained for at least 2 years and made available to consumers upon request.

In the documents supporting the proposed regulations, the Attorney General acknowledges the regulatory cost to the State will be $4.7 million for FY 2019-2020 and $4.6 million for FY 2020-2021. The estimated cost to business between 2020

and 2030 is said to be $467 million to $16,454 million. The documentation goes on to acknowledge there is a potential competitive disadvantage for California companies (the estimate is 15,000 to 400,000 businesses will be impacted) to companies which operate outside California and are not otherwise subject to the CCPA. For that reason, submissions proposing alternate means of implementation are requested which address the following topics:

1. The establishment of differing compliance or reporting requirements or timetables that take into account the resources available to businesses.

2. Consolidation or simplification of compliance and reporting requirements for businesses.

3. The use of performance standards rather than prescriptive standards.

4. Exemption or partial exemption from the regulatory requirements for businesses.

A business is exempt if it does not and will not sell (bearing in mind the broad definition of “sell”) consumer personal data and so states in its privacy policy. If exempt, the opt-out logo is not required.

If a company has a loyalty or other financial incentive program, those are still permitted, but there are specific notice requirements which generally mirror the criteria mentioned above regarding what must be included in the notice and how those incentives are to be explained. Similarly, if any cost or service differences do apply, they must meet the standard and also provide a “good-faith estimate” of the value of the consumer data which forms the basis for the differential, and also a description of the method used to calculate the value stated.

Given these regulatory mandates, here are some additional factors for business to consider:

1. How will you give the required notice to consumers?

2. What form will the update to your privacy policy take?

3. Are you required to provide an opt-out option and the corresponding logo?

4. Do you reflect the last date updated on your privacy policy?

5. Do you provide a contact for more information?

6. The requirement is two or more designated methods for the consumer to request data, to include a toll free telephone number, a link or form on the website, a designated email address, a form submitted in person or a form submitted through the mail. Which of these do you currently provide? How does the business usually interact with consumers? Where on the list of methods of notice do your usual means of consumer interaction fall?

7. Deletion requests are subject to two steps; first, the consumer submits the deletion request and then separately confirms deletion is desired. How will you

implement this process?

8. If the consumer submits a request in other than a proscribed method, the company must decide whether it will treat the request as properly submitted or provide instructions to the consumer as to how to submit his/her request or remedy any deficiency. Which will you opt for?

9. Businesses must respond to requests within 45 days, but must confirm receipt within 10 days and confirm how the business will process the request and when it expects to provide a substantive respond. While verification of the identity of the requestor is permitted, the response time clock starts at time of receipt, not when the verification is completed. Businesses are barred from disclosing a Social Security, driver's license, or other government issued identification number, along with the financial account, health insurance or medical identification number, an account password or security questions and answers. Generally individualized responses are required. How will you implement this mandate?

10. If the request is to delete, the business may respond by erasing the data from its systems or by de-identifying or aggregating the data unless the business determines to not comply with the request. If so, it is then necessary to provide that response to the consumer along with the grounds for refusal. The business may also offer the consumer the ability to delete selected portions only if the global option is also offered and more prominently displayed. How will you implement this requirement?

The CCPA regulations also go on to address the use of service providers (third parties) which owe duties of indemnity and compliance to the businesses which hire them (and conversely the business owes a duty of indemnity to that service provider), dealing with the collection and use of the data collected. There are also general rules for verification of consumers, password protected accounts, non-account holders and authorized agents.

Clearly these regulations are complex and demanding. Companies would, therefore, be well-served to first make sure as to the specifics of their business model, the nature and extent of the personal data collected, and how that data is used and shared. A refresher to be sure the information in hand is current is recommended before proceeding further. Once all of that is clear, a carefully study of the requirements of the CCPA regulations is in order, so as to compare those requirements with current practices, and then, of course, update accordingly.

Bearing in mind individual and class action lawsuits are now permitted, someone is going to be the poster child for having messed up compliance. Whether you handle implementation yourself or we or another advisor assist you, getting it right the first time is critical to having a peaceful holiday season! Will you be ready?