NOW + NEXT

PRIVACY LAW ALERT | NIXON PEABODY LLP

OCTOBER 15, 2019

California attorney general issues proposed regulations under the California Consumer Privacy Act of 2018

By Karl Belgum

The California Consumer Privacy Act ("CCPA" or the "Act") was passed in June 2018 and goes into effect on January 1, 2020. It includes a list of topics which the attorney general of California is mandated to clarify through regulation, and gives him carte blanche to issue any regulations "necessary to further the purposes of this title." (Civ. Code 1784.185.) On October 9, 2010, the attorney general issued his long-awaited proposed regulations. Hearings have been scheduled for four locations in California on December 2–5, 2019. Written comments are due by December 6.

The attorney general's Initial Statement of Reasons that accompanies the proposed regulations declares that they were drafted to "provide clear direction to business." The resulting document is 9,300 words long, almost the length of the original Act. The Act and regulations together are now approximately four times as long as the entire original United States Constitution. The regulations set forth specific requirements as to the drafting of notices, the contents of web pages and privacy policies, and the procedures to follow in responding to consumer requests to disclose or delete personal information as well as opt-out and opt-in requests. Every business holding personal information (paper or electronic) regarding California consumers will need to develop a plan to comply with this complex new regulatory scheme.

Notices to consumers

The Act is full of notice requirements, and the regulations seek to further clarify and define them. In general, the regulations require that notices be given clearly, and in any language in which the business typically communicates with customers (including through advertising). Under the Act, notice of consumer rights must be given at or before the point data is collected from a consumer. The regulations specify that such notice must include the opt-out link already described in the statute. They also specify that a business must explicitly state if it does not collect personal information, and also provide that a company cannot change its mind about the sale of data once the data is collected pursuant to such a declaration. In a nod to business efficiency, an online notice at the point of data collection can merely link to the privacy policy, making the terms somewhat easier to update. However, the regulations include onerous provisions for "data brokers" who sell

personal information to confirm that such information was originally obtained pursuant to the correct notices and opt-out rights.

Opt-out rights

The regulations specify how businesses should allow consumers to exercise their opt-out rights, providing somewhat different options tailored for various types of businesses. Specifically:

- Small businesses with no websites can use a non-website method,
- "Main Street" business who may have a website but who have substantial off-line interactions with their consumers can provide an off-line method to opt out, and
- Online businesses can use opt-out functions on their websites.

The regulations clarify that a consumer who clicks on the required "Do Not Sell My Personal Information" button on the web page (or at the point of sale) should be taken directly to a page where the opt-out choice can be made. A business is excused from having an opt-out choice if its privacy policy says it does not sell personal information, but then it has to abide by that promise.

Privacy policies

The proposed regulations indicate that the business's privacy policy—which may be a California-specific policy—should provide all the information necessary to disclose a consumer's rights under the Act and how to exercise them, including how to appoint an "agent" to exercise the consumer's rights on his or her behalf, and a contact point to answer questions about privacy issues. In a provision clearly targeted at high-profile internet businesses, the Act requires any business that buys, receives, sells, or shares the information of over four million consumers (ten percent of the state's population) to post metrics online regarding the number of consumers making requests to disclose or delete data or opt out of sales, and the business's track record in responding to such requests, as well as its policies for training staff to comply with the law.

Submitting a request

One of the most troubling aspects of the Act is its requirement that a business disclose personal information to those who request it, while at the same time making sure the request is "verified." This obviously puts businesses in a difficult spot, subject to liability for not disclosing as well as for disclosing it to the wrong person. The same issue applies to requests to delete information. The attorney general was tasked with defining by regulation what constitutes a verified request. The proposed regulations specify that a business must allow two methods to make a request to disclose or delete information. Businesses with websites can use an online form for these requests, but an email address or a form submitted by mail or in person may also be used. Regardless, the methods should tie to the way the business ordinarily interacts with its customers. Requests to delete must use a two-step process, in which the consumer confirms the original request. A business that does not interact directly with consumers must make an online method available for requests.

Responding to a request

The regulations contain extensive provisions regarding how a business should respond to a request to disclose or delete personal information. The business must acknowledge the request within ten days and respond substantively within 45 (with a possible extension). If a business cannot verify that the request to disclose information is coming from the consumer who purports to make the

request, it cannot disclose "specific pieces" of information but may still disclose "categories." Or, alternatively, it can disclose its "general business practices" for collecting, maintaining, and selling information. Certain categories of high-risk information are exempt from disclosure requests altogether, such as social security numbers, driver's license, financial accounts, insurance, account passwords, or security question answers. Businesses with secure internet accounts must allow "self-service" access to personal information through such accounts. The regulation makes clear that to disclose "categories" of information means to provide details on the specific categories related to the particular consumer, not just a cross reference to the company' standard policies for collecting or using data.

Guidance is also provided on responding to requests to delete information. A two-step confirmation process must be used to make sure the consumer clearly wants the data deleted. Such requests can be denied if the consumer's identity cannot be verified. Deletion of information on backup systems can be deferred until the systems are next accessed in the ordinary course. A business can respond by deidentifying or anonymizing the data, but it must tell the consumer how it responded.

Service providers

The regulations clarify the responsibilities of "services providers," and state that service providers working for nonprofits or governmental enterprises outside the scope of the Act are not governed by its provisions.

Requests to opt out

The proposed regulations contain extensive provisions regarding making and responding to requests to opt out of the sale of personal information. Two methods will be provided to opt out, one of which will be the Do-Not-Sell-My-Info link on the webpage. As with the methods for requesting disclosure or deletion, the opt out methods should tie to the business's usual methods for communicating with its customers. Browser settings must be accepted as a way to communicate do-not-sell requests. A business receiving an opt-out request must give notice to the other businesses to which it sold the information in the last 90 days, which then imposes on them the duty not to sell it. Opt-out requests need not be verified, but can be denied if considered fraudulent. Consumers who have opted out can opt back in to allow sale of their information through a two-step process, and they can be told that a given transaction requires opt-in permission as a condition of the transaction.

Training

The regulations provide guidance on how businesses must train their employees to comply with the statute and require that records be kept of consumer requests and the responses made.

Household information

The Act generated confusion by including "household" information within the definition of personal information, resulting in concern that one member of a household may access or demand deletion of the information of other household members. The regulations state that a business may respond to a request to know or delete household information by providing only "aggregate data," unless all the members of the household join in a verified request. If the consumer makes the request through a password-protected account, the business can respond as to information linked to that account without worrying about whether it is household data or not.

Verification

The regulations specify how a business can verify the identity of someone making a request to disclose or delete information. This is one of the subjects that the Act requires the attorney general to address in regulations. The verification regulations fall into two categories: (i) password protected accounts and (ii) other information. For password protected accounts, businesses can generally rely on their existing account log-in verification procedures. For others, they have to devise a "reasonable" verification system based either on matching the consumer's verification with existing data on file at the business, or they must hire an independent verification service. The regulations prohibit a business from retaining the categories of personal information listed in the existing data security law (Civ. Code 1798;81.5 – Social Security, credit card, driver's license, etc.) unless needed for verification purposes. If a business asks for additional personal information as part of the verification process, it cannot keep it for other uses.

A consumer with no account relationship at all can still request disclosure or deletion of his or her personal data, but to obtain disclosure of categories of information the consumer must provide two pieces of information that match what is on file at the company, while a request to disclose specific pieces of information must provide information that matches three pieces of information on file at the company, plus a signed declaration, which the business must keep on file. As an example, if a request to disclose or delete is made by a customer who used a credit card to make a purchase at a store with which the customer has no account relationship, the business could ask for the security code on the back of the card plus information about recent purchases as a form of verification. A business can exempt itself to some extent from the verification and disclose/delete obligation if there is no reasonable method for it to verify the identity of consumers as to some aspects of the information it holds; however, it must explain why that is so on its privacy policy. Overall, the onerous and unwieldy provisions regarding verification of requests create an enormous incentive for businesses not to retain sensitive categories of personal information in an identifiable form.

Use of agents

The proposed regulations put significant limits on the use of agents to make requests to disclose or delete. Absent an actual power of attorney under the Probate Code, the individual consumer must still verify his or her identity with the business as if they were making the request themselves. And the agent has to prove that it is authorized. This renders the whole concept of using an agent to make requests highly unwieldy.

Minors

The Act requires affirmative opt-in by minors between 13–16, and opt-in by a parent or guardian for minors below 13, before personal information of such minors can be sold. Those provisions pose significant problems to businesses because of the need to verify in a reliable way how old the consumer is. For children under 13, the regulations borrow the verification practices mandated by the Federal Trade Commission pursuant to the Children's Online Privacy Protection Act ("COPPA"). The parent can use a credit card, provide a government ID, or speak with someone on a toll-free line. For children 13–16, the business must simply adopt a reasonable procedure to verify the opt-in request, and must advise the minor of his or her right to opt out later, and how to do it.

Discrimination and financial incentives

The Act somewhat inconsistently bars discrimination in price, quality, or service based on the exercise of consumer privacy rights but also allows businesses to give "financial incentives" to allow the sale or use of personal information as long as they are not abusive. The legislature left it to the attorney general to clarify this inconsistency through regulation. The result is not entirely successful. The proposed regulations define a "price or service difference" to include a "financial payment" but also define "financial incentives" to include "payments to consumers." A clear line is still not drawn between the two concepts. The regulations do specify that consumers must get a comprehensible notice about any incentive program, including the categories of information involved, the value of the information to be exchanged, and a description of how the business calculated the value. This portion of the statute, and the proposed regulations, marks the beginning of a move toward creation of a market in consumer personal information.

In response to comments received from business, the regulations provide examples of how a merchant can operate a loyalty program without running afoul of the Act. The terms of any incentive program can be set forth in a separate document, not in the privacy policy, so that they can be changed over time with respect to different promotions. The regulations also tackle the difficult question of how to determine whether a difference in price or service bears a reasonable relationship to the value of the consumer's data which is the subject of the bargain. The regulations clarify that the value in question is the value of the data to the business that is acquiring it, and that the test should be objective, not subjective (i.e., the fact that a consumer says they put a very high value on their information is not dispositive). The regulations recognize that there is no accepted methodology for calculating the value of consumer data, and therefore allow for any method that is "practical, reliable, and used in good faith," but the regulations also give specific examples of ways that value may be determined, including either calculating the total value of all consumer information and then dividing by the number of consumers, generating an "average value," or attempting to calculate the value of one additional consumer's data, which the regulations refer to as a "marginal value." The guidance is quite general; however, the main point is that the regulations leave a lot of flexibility to businesses in coming up with any defensible method.

Conclusion

The proposed regulations attempt to alleviate the burden on businesses in some ways, but their sheer volume and complexity will impose a burden in any event, as businesses plan to comply with the statute by January 1, 2020. The one theme that comes through is the need for businesses to keep as little personal information as possible, to maintain it in deidentified or aggregate form if at all possible, to come up with a defensible strategy for verifying requests, and to plan for how the business will handle requests to disclose or delete when they inevitably arise.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Karl Belgum at **kbelgum@nixonpeabody.com** or 415-984-8409
- Christopher Mason at **cmason@nixonpeabody.com** or 212-940-3017
- Jason Gonzalez at **jgonzalez@nixonpeabody.com** or 213-629-6019
- Daniel Deane at **ddeane@nixonpeabody.com** or 603-628-4047
- Jenny L. Holmes at **jholmes@nixonpeabody.com** or 585-263-1494