Cybersecurity Law Report
An Acuris company

cslawreport.com

September 9, 2020

STATE LAWS

Implementing the CCPA Regulations: Are You Ready?

By Amanda R. Lawrence, Elizabeth E. McGinn and Sherry-Maria Safchuk, *Buckley*

The final regulations under the California Consumer Privacy Act, introduced by the California Attorney General last October, became effective on August 14, 2020. The AG has already implemented many of the changes suggested in the public comments, but there are still several open questions that businesses are grappling with as they implement the regulations. This article discusses potential implementation issues and considerations for businesses as they work to incorporate the CCPA regulations in their business privacy practices.

A new law, the California Privacy Rights Act of 2020 (the CPRA), a modified version of the CCPA, will appear on the November 2020 ballot in California and passage seems imminent, adding to a company's compliance burden under the CCPA. Businesses need to monitor the CPRA and identify how the changes between the CCPA and the CPRA will impact a business's privacy practices.

See CSLR's two-part series on the CCPA and online ads: "Facebook Finally Acts, AG Starts Enforcement" (Jul. 29, 2020); "Contract and Compliance Consequences" (Aug. 5, 2020).

Providing CCPA Notices

The CCPA requires four notices: (1) a CCPA privacy policy, (2) a Notice at Collection, (3) a Notice of Right to Opt-Out and (4) a Notice of Financial Incentive. For each of these notices, the CCPA regulations set forth general principles that apply to all notices. At first glance, the CCPA regulations may appear to provide some instructions for presenting the various notices, but they do not provide further guidance as to actual compliance with the principles, nor do they provide model forms or sample language, the lack of which may present compliance challenges.

The CCPA regulations also set forth additional principles for the privacy policy and the notice of financial incentive.

Presentation and Language Requirements

The general principles state that the notices must be "designed and presented in a way that is easy to read and understandable to consumers" and that the notice must use "plain, straightforward language" and avoid "technical or legal jargon."

However, the AG removed references to the "average" consumers from the presentation requirements, likely because of public comments regarding the meaning of this term, but the AG's expectations are unclear and businesses likely will grapple with whether a given notice is easy to read and understand by a specific consumer, and whether the

disclosure is "plain" and straightforward." Drafting a consumer-friendly privacy policy becomes even more difficult when a business's data collection is complex and the business must explain such collection practices to consumers.

Formatting

The notices must be in a "format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable." The regulations, however, do not provide examples of formatting or placement of the notices that would comply with this requirement. Further, what may draw the attention of one consumer may not be the same for another consumer. This is an area where businesses may need to be creative with how they present the notices to consumers.

Foreign Language Requirements

The notices must be available in the languages in which the business in its ordinary course provides certain information to California consumers. Businesses, in response to prior versions of the regulations, asked the AG to clarify that compliance with the CCPA would not require a business to translate a disclosure and, if a disclosure needed translation, requested that the AG approve disclosure forms in acceptable translations.

The AG declined to revise the requirement based on these comments because it took the position that "businesses that in the ordinary course provide materials and information in different languages should be able to accurately translate their notices and disclosures." Thus, if a business is currently translating disclosures into other languages in California, it may need to consider whether it should do so with respect to CCPA notices.

Accessibility Requirements

The notices must be reasonably accessible to consumers with disabilities. The CCPA regulations direct businesses to comply with generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium. When notices are provided offline, the business must provide information on how a consumer with a disability may access the notice in an alternative format.

The Web Content Accessibility Guidelines provide a number of recommendations for making web content more accessible to a wide range of people with disabilities. Businesses should consult and implement the guidelines to ensure that people with disabilities who visit their websites are accommodated. This may be an area on which plaintiff's attorneys may focus (*i.e.*, violation of the CCPA for failure to comply with access requirements) in light of their increased focus on violations of the Americans with Disabilities Act.

See CSLR's two-part series on CCPA litigation: "How to Stem the Coming Tide" (Jan. 22, 2020); "How to Avoid Claims Under Other Statutes" (Feb. 5, 2020).

Responding to Requests

Another challenging task for companies may be responding to requests.

Responding to Requests to Know Specific Pieces of Information

The CCPA requires that a business respond to a request to know specific pieces of information by disclosing and delivering personal information "in a portable and, to

the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance." In another section of the CCPA, the rule reiterates that the disclosure of personal information must be "in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance."

Formatting

The regulations do not address how a business may provide the personal information requested in a "portable" and "readily useable format." While the regulations address instances when a business maintains a password-protected account with the consumer by repeating the requirements in the CCPA, they do not address how a business should respond to a request to know specific pieces of information if it does not maintain a password-protected account with the consumer. Rather, the regulations merely provide that "[a] business shall use reasonable security measures when transmitting personal information to the consumer" without further guidance on what "reasonable security measures" entail.

Based on the foregoing guidance, businesses are left to grapple with what format should be used to identify the specific pieces of personal information in response to a request and how it should securely transmit the information to a consumer. Businesses will need to work with their information technology departments to determine the best format for disclosing the specific pieces of personal information. In determining "reasonable security measures," businesses may wish to consider regulatory guidance and industry standards to determine whether the business needs to implement or supplement its data security procedures and processes to ensure that CCPA disclosures are securely transmitted.

Verification

In addition to figuring out how to disclose and deliver the personal information to the consumer, the business will first need to verify the consumer. The regulations provide scant guidance regarding verification aside from providing general rules, which lay out considerations for the business, and set forth limited instruction regarding verification for password-protected accounts and non-account holders. The regulations prohibit disclosure of certain sensitive information (*e.g.*, Social Security number, driver's license, financial account number, health insurance or medical identification number, account password, etc.), but failure to properly verify a consumer may give rise to significant exposure (*e.g.*, reputational risk, litigation risk) and may result in implications beyond the CCPA, especially if the disclosure results in identity theft, domestic violence or stalking.

A business may verify a consumer's identity through the business's existing authentication practices for password-protected accounts. Certain businesses may have robust authentication practices in light of the sensitivity of the information collected and maintained, but other businesses will need to update their authentication processes to ensure that a consumer is adequately verified. The regulations for non-accountholders set forth a different standard of verification depending on the request. The standard for certain requests to know the categories of information and requests to delete, is a "reasonable degree of certainty," which requires a business to match at least two data

points provided by the consumer with data points maintained by the business. However, for requests to know specific pieces of information and certain requests to delete, the standard is a "reasonably high degree of certainty," which requires the business to: (1) match at least three pieces of personal information provided by the consumer with personal information maintained by the business, and (2) obtain a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is subject to the request.

The regulations provide an example in the retail context, but the example is not helpful in other contexts. If a business collects a consumer's full name, IP address, location information and inferences when the consumer interacts with the business online, the business may have a difficult time identifying the personal information it must collect from the consumer for verification purposes because such a consumer likely is not aware of their IP address, location information and the inferences the business identified during the consumer's browsing session. Thus, depending on the volume of requests, businesses may need to tailor their approach to verification based on the request, while ensuring that the verification method aligns with the requirements of the regulations. Further, if a business receives a request for specific pieces of information, it may need to verify the consumer under both verification standards. Specifically, if a business cannot verify the identity of the consumer making a request for the disclosure of specific pieces of information under the reasonably high degree of certainty standard and the request is denied, the business also must evaluate the consumer's request as if the consumer requested the categories of personal information and verify the consumer's request according to the lower "reasonable degree of certainty" standard.

Thus, for requests for specific pieces of personal information, a business must create a process for verifying consumers under two standards if the consumer does not meet the higher standard.

Responding to Requests to Know or Delete Household Data

The definition of personal information under the CCPA is broad enough to include information that identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular "household." The regulations further define a "household" as a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business and (3) are identified by the business as sharing the same group account or unique identifier.

Thus, if a business receives a request for household data, it will be required to parse through the personal information of the persons in the household to determine whether such information is considered a consumer's personal information or the household's personal information. This may be more difficult to do in larger households consisting of several roommates (*e.g.*, student housing). To prepare such an analysis, it will be important for a business to have clear policies and procedures differentiating between household and consumer personal information because failure to do so may result in a business inadvertently disclosing consumer personal information to the household or deleting consumer personal information.

The regulations further address how a household may submit a request to know or delete household information. If the consumer has a password-protected account by which it provides the business household personal information, the business may process requests to know and requests to delete relating to household information through the business's existing business practices if in compliance with the CCPA regulations. If a household does not have a password-protected account with a business, three conditions must be met before the business may comply with a request to know specific pieces of personal information or a request to delete:

- all consumers of the household jointly request to know specific pieces of household information or the deletion of household personal information;
- the business individually verifies all the members of the household subject to the regulation's verification; and
- the business verifies that each member making the request is currently a member of the household.

Since the regulations do not provide instructions for how a household may jointly request to know or delete and how the business must verify that each member is currently a member of the household, businesses should ensure that they allow consumers to submit a request to know or request to delete specific pieces of household personal information if the business collects such household personal information.

Further, in addition to confirming that all household members have jointly submitted a request, when verifying the household, businesses will need to implement a two-step verification process: (1) verification of each consumer's identity; and (2) verification that each consumer is a current member of the household. If the business is unable to verify any of the consumers based on the higher standard in response to a request to know specific pieces of information, the regulations specific to household information are silent as to whether the business also must verify the consumers as if the household is seeking the disclosure of the categories of personal information.

A business may thus be required to verify each consumer in the household based on the lower standard of verification even though the regulations do not expressly require a business to perform such an analysis with respect to household data.

Consumer Experience

It is important for businesses to focus on compliance with the CCPA and its implementing regulations, but businesses must not lose sight of the consumer experience. If consumers become frustrated, they could voice their concerns to the business or a regulator. This is especially true in the privacy context when personal information is at stake. Under the CCPA, consumers have several rights with respect to their personal information and to exercise those rights, they will need to reach out to the business. A business complying with the CCPA should pay particular attention to how it allows consumers to submit requests and how it will respond to such requests. If the consumer must provide a significant amount of information to submit a request or for verification purposes, the consumer experience will be impacted and may result in consumer complaints or regulator scrutiny. Thus, businesses should consider the following issues.

Training

The CCPA and its regulations require that all individuals responsible for handling consumer inquiries about the business's privacy practices or CCPA compliance be trained on the CCPA requirements and how consumers can exercise their rights. A business' training program should focus on how customer service representatives can make the process easier for the consumer. This likely will require open communication between the consumer and the business as well as transparency regarding the request and response processes. Thus, businesses should consider providing their customer service representatives with scripts, templates and procedures, and to run practice scenarios with such employees to assist them with elevating the consumer experience.

Streamlining Request Process

A businesses should review its request process to ensure that it is not asking the consumer for too much information for purposes of verifying the consumer's request. While there is specific information that the business must obtain to verify a consumer, there are ways to make the process more consumer-friendly, such as using an interface/webform that is easy to understand and navigate, incorporating formatting to break up questions and requesting the information at one time instead of piecemeal.

Verification Methods

The manner in which the consumer is verified also will impact the consumer experience. If the verification process is cumbersome, the consumer experience will suffer. As such, businesses will need to walk a fine line to comply with the verification requirements and maintain a consumer's privacy while ensuring that the consumer does not become frustrated while trying to exercise their privacy rights.

See CSLR's three-part guide to cybersecurity training: "Program Hallmarks and Whom to Train" (Oct. 16, 2019); "What to Cover and Implementation Strategies" (Oct. 23, 2019); and "Assessing Effectiveness and Avoiding Pitfalls" (Oct. 30, 2019).

Bridging the Gap

As businesses update their processes, some creativity will be required to bridge the gap between the requirements of the regulations and practical implementation. The CCPA permits a business or third party to seek the AG's opinion on compliance with the CCPA, but it is unclear how often the AG will exercise this authority and businesses may, instead, begin to see regulation by enforcement. The AG also has identified areas in the CCPA where further analysis is required, such as the definitions of "business," "business purpose," "sale," "service provider," and "third-party" requirements related to the Notice at Collection, the opt-out button or logo, the privacy policy, the manner in which consumers submit requests online and responding to requests and the requirements related to opt-outs. Thus, business may see updates or guidance issued with respect to these requirements.

Amanda R. Lawrence is a partner at Buckley LLP, where she assists clients in managing cybersecurity, privacy, information security and vendor risks and compliance, as well as evaluating and addressing potential data security incidents, including drafting consumer and regulator notifications. She is a frequent author and lecturer on litigation

and compliance issues in financial services, including privacy, cybersecurity, data breach, mortgage origination enforcement and litigation, RMBS, class actions and FTC and other regulator priorities.

Elizabeth E. McGinn, a partner at Buckley LLP, focuses her practice on assisting clients in identifying, evaluating and managing the risks associated with cybersecurity, internal privacy and information security practices, as well as those of third-party vendors. A significant part of her practice involves addressing data security breaches, working proactively with clients to prevent data security breaches and responding to regulatory inquiries, investigations and enforcement actions related to privacy, information security and cybersecurity issues.

Sherry-Maria Safchuk is counsel in the Los Angeles office of Buckley LLP, and assists clients on privacy issues, including those related to the CCPA. She represents clients in regulatory and compliance matters and provides support for complex litigation and government investigations involving the mortgage, consumer and commercial lending industries.