LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
THURSDAY, MAY 12, 2022

MCLE

CPRA series: Part III - Notice and disclosure obligations

By Ron Raether, Kim Phan, Grady Howe, Lissette Payne and Sadia Mirza

As we explained in an earlier installment, most privacy laws derive from the Fair Information Practice Principles (FIPPs). The FIPPs provide, in part, that consumers should be given notice of how their information will be used and shared, before their personal information is collected, to allow consumers to make an informed choice.

The California Consumer Privacy Act of 2018 (CCPA) imposes several notice and disclosure obligations on covered businesses. While the California Privacy Rights Act of 2020 (CPRA) did not modify when businesses are required to provide notice, it did make several important changes to the CCPA, which include changes to the following:

Updates to Notice at Collection

The CCPA requires that businesses provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, and the purposes for which the personal information will be used ("Notice at Collection").

The CPRA increases the amount of information that must be provided in the Notice at Collection. Prior to Jan. 1, 2023, the effective date of the CPRA, businesses will need to update their notices at collection to address the new and modified information to be provided to consumers. Under the CPRA, information provided in the Notice at Collection must include the following:

(1) Whether the collected personal information is sold or shared. Under the CCPA, companies that sold consumers' personal information data must disclose that practice. Under the CPRA, the definition of "selling" remains the same as it was under the CCPA, which includes various forms of sharing/disclosures of personal information by a business to another business or third party for valuable consideration. However, the CPRA extends the Notice at Collection disclosure obligations to include whether any categories of personal information are shared. Notably, the definition of "sharing" includes any disclosure of personal information for "cross-context behavioral advertising," which includes targeted advertisements based on a consumer's interactions with other businesses, websites, applications, or services. For further information on selling and sharing (and the distinction between the two), please see Part 2 of this series.

(2) Sensitive Personal Information. Under the CCPA, businesses must include in the Notice at Collection the categories of personal information collected about consumers. The CPRA creates a new category of personal information – "sensitive personal information." As such, under the CPRA, the Notice at Collection disclosure obligations are extended to include the categories of any sensitive personal information collected and the purposes for collection of such sensitive personal information.

(3) Data Retention. Under the CPRA, businesses must include in their Notice at Collection the length of time each category of personal information, including sensitive personal information, will be retained. If it is not possible to state how long the data will be retained, businesses must include the criteria used to determine the retention period. Either way, no personal information is allowed to be retained for longer than is reasonably necessary for the disclosed purpose in the Notice at Collection.

From a practical perspective, the modifications to the Notice at Collection will require many businesses to revisit their data maps to ensure they are capturing the information not previously required by the CCPA (i.e., sensitive personal information, data retention periods, whether information is being "shared," etc.). While there is still some hope the CPRA will exclude personal information collected in the employment context (see Part One for additional information), businesses should plan on reviewing their Notices at Collection relating to employee data to determine what modifications will be required, if any.

Updates to Notice of Financial Incentive

Under the CCPA, a business must disclose the material terms of any financial incentive the business offers to consumers as compensation for the collection or sale of personal information. The CPRA extended this disclosure obligation to also include the material terms of any financial incentive the business offers to consumers for the sharing or retention of their personal information as well.

Updates to Privacy Policy

Under the CCPA, businesses' privacy policies must provide a comprehensive list of their online and offline practices regarding the collection, use, disclosure, and sale of personal information, as well as the rights of consumers regarding their personal information. Additionally, businesses must develop and post a privacy policy that informs consumers about the existence of, and guidance on how to exercise, their CCPA rights.

The CPRA modifies certain rights provided for in the CCPA, while also adding several others. The extended and additional rights include:

(1) Right to opt out of the sale and sharing of personal information. As mentioned above, the CPRA requires a business to provide a notice to inform consumers of their right to direct a business that "sells" their personal information to stop selling their personal information. Information on the right to opt out of the sale as well as the new right to opt out of the sharing of personal information, and the method for exercising these rights, must be included in a CPRA compliant privacy policy.

Furthermore, under the CCPA, a business that sold consumer data must disclose that information and include a "Do Not Sell My Personal Information" link on its homepage. Accordingly, the CPRA adds that the "Do Not Sell" link referenced above must be edited to "Do Not Sell or Share My Personal Information."

With regards to the sharing of consumers' personal information,

Reprinted with permission from the *Daily Journal*. ©2022 Daily Journal Corporation. All rights reserved. Reprinted by ReprintPros 949-702-5390.

the CPRA also requires that the privacy policy disclose a list of the categories of personal information it has sold or shared about consumers in the preceding 12 months by reference to the enumerated category or categories that most closely describe the personal information sold or shared, or if the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall prominently disclose that fact in its privacy policy.

(2) Right to limit the use and disclosure of sensitive personal information. The CPRA requires businesses, upon request by a consumer, to limit the use and disclosure of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services. Businesses that use and disclose sensitive personal information for any other purpose must provide consumers with the ability to opt out of such use and disclosure.

(3) Right to Correct/Rectification. The CPRA provides consumers the right to request that inaccurate information held on them is corrected. Information on the right to correct/rectification, and the method for exercising this right, must also be included in the privacy policy.

The CCPA regulations, 11 CCR §§ 999.308, had also expanded the content to be included in privacy policies, which were enacted into law by the CPRA by requiring in the statute that privacy policies include the following information:

(1) The categories of sources from which consumers' personal information is collected.

(2) The business or commercial purpose for collecting or selling consumers' personal information, and under the CPRA also for sharing consumers' personal information.

(3) The categories of third parties to whom the business discloses consumers' personal information.

The CPRA did not otherwise impact the other content requirements for privacy policies as set forth in the CCPA regulations.

Disclosure Updates in Response to Requests to Know

The CCPA allows consumers to submit a "Request to Know" for a business to disclose its collection and treatment of the consumer's personal information during the past twelve months, which includes the following:

(1) The categories of personal information the business collected about the person;

(2) The categories of sources from which the personal information was collected;

(3) The business or commercial purpose for collecting or selling the personal information;

(4) The categories of third parties with whom the business shares personal information; and

(5) The specific pieces of personal information it has collected about that consumer.

The CPRA modifies these disclosures in the following ways:

(1) Businesses must now provide information about the business or commercial purpose for sharing personal information. "Shared" is defined as providing personal information to a third party for cross-contextual behavioral advertising.

(2) Clarifies that if the consumer requests that the business disclose the required information beyond the 12-month period, then the business shall be required to provide that information unless doing so proves impossible or would involve a disproportionate effort. This change will only apply to data collected on or after January 1, 2022.

(3) Directly requires service providers and contractors to aid businesses in responding to a verifiable consumer request.

(4) Clarifies that businesses must provide specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance.

(5) Clarifies that personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.

Changes to Opt-Out Preference Signals

The CPRA contemplates the creation of an "opt-out preference signal," which would indicate consumers' intent to opt-out of a business' sale or sharing of their personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both. The CPRA indicates that the signal would be sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in future regulations. Businesses would be able to elect whether to utilize opt-out links or the opt-out preference signal to satisfy their CPRA obligations. The CPRA does not clearly define an "opt-out signal," but time will tell if it will be treated as synonymous with what was described in the CCPA regulations as a "user-enabled global privacy control." There, the CCPA regulations defined such a mechanism as "a browser plug-in or privacy setting, device setting, or other mechanism that communicates the consumer's choice to opt-out."

What to Expect from Anticipated Regulations?

As discussed in the previous installments of this series, the California Privacy Protection Agency is now responsible for updating existing regulations and adopting new regulations concerning the CPRA. Relevant to notice and disclosure obligations, the CPPA is expected to issue regulations to:

(1) Ensure that the notices and information are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer;

(2) Define the term "specific pieces of information obtained from the consumer" with the goal of maximizing a consumer's right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful to the consumer, including system log information and other technical data;

(3) Require businesses' response to access requests to include meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer; and

(4) Harmonize the various notices to consumers to promote clarity for consumers.

The timeline for adopting these new regulations under the CPRA was set for July 1, 2022. The CPPA has already stated that it will miss the deadline. Under the CCPA, businesses had almost two years between when the CCPA was enacted and when the Attorney General was empowered to bring enforcement actions for CCPA non-compliance. Similarly, the CPRA provides businesses a little more than two years to adjust their existing practices to comply with the new obligations in the law. On Jan. 1, 2023, the CPRA will go into effect. Beginning July 1, 2023, the CPPA will begin enforcing the new obligations added by the CPRA. By this date, business notices, policies and other required disclosures should be fully compliant with the requirements of the CPRA to avoid the risk of an enforcement action. However, it remains to be seen when the regulations will be finalized, including when businesses will be required to comply with any such regulations.

Ron Raether and Kim Phan *are partners, and* **Grady Howe, Lissette Payne** *and* **Sadia Mirza** *are associates at Troutman Pepper Hamilton Sanders LLP.*

Reprinted with permission from the *Daily Journal*. ©2022 Daily Journal Corporation. All rights reserved. Reprinted by ReprintPros 949-702-5390.