LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Insights And Omissions From Calif. Privacy Rules Draft

By **Cassandra Gaedt-Sheckter, Alexander Southwell and Ryan Bergsieker**
(July 8, 2022, 5:28 PM EDT)

Cassandra Gaedt-Sheckter

Alexander Southwell

Ryan Bergsieker

The California Privacy Protection Agency released its much-anticipated draft regulations for the California Privacy Rights Act at the end of May, marking a significant step toward full implementation of the most comprehensive state privacy legislation in the U.S.

The draft regulations provide additional clarity on certain aspects of the law and insight into the agency's priorities, while also arguably adding new requirements beyond the scope of the CPRA and leaving out significant regulations that businesses have been eagerly awaiting.

This release is the first step in a multipart rulemaking process that extends well past the initial target for finalizing regulations of July 1.

We analyze here a few highlights from the draft regulations, as well as two notable omissions.

Despite being subject to change, and not comprehensive, the regulations still provide helpful guidance for businesses working on enhancing their compliance programs before the CPRA takes effect Jan. 1, 2023.

Dark Patterns

Unlike its predecessor statute, the California Consumer Privacy Act, the CPRA seeks to address issues relating to dark patterns, which the CPRA defines as "[a] user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation."

The draft regulations indicate that any dark patterns used to obtain consent violate the law and vitiate any consent provided. In explaining how consent may be obtained, the regulations provide five principles that can help guide businesses in creating consent flows, requiring the user interface to:

- Be easy to understand;

- Provide symmetry in choice;
- Avoid confusing language or interactive elements;
- Avoid manipulative language or architecture; and
- Be easy to execute.

The draft regulations also provide examples of alleged dark patterns, including interfaces that many consumers see in everyday internet usage. For example, the draft regulations state that "[w]hen offering a financial incentive, pairing choices such as, 'Yes' (to accept the financial incentive) with 'No, I like paying full price' or 'No, I don't want to save money,' is manipulative and shaming."

With respect to cookie preference centers, the draft regulations state that "[a] website banner that serves as a method for opting out of the sale of personal information that only provides the two choices, 'Accept All' and 'More Information,' or 'Accept All' and 'Preferences,'" is explicitly not permissible for opting out of the sale or sharing.

Service Providers, Contractors and Third Parties

Service Providers and Contractors

The draft regulations include several new provisions affecting service providers and contractors, but for ease of reference and given the similarity between the two categories, we will use the term "service provider," i.e., entities that collect and process data in the context of providing a service to another entity.

The changes expand the applicability of the CPRA. They permit service providers to use information for product or service improvements, and institute specific requirements for contracts governing the relationship between the business and service provider.

First, liability as a service provider is expanded. The draft regulations state that they still will apply when a vendor "provides services to a person or organization that is not a business, [but] would otherwise meet the requirements and obligations of a 'service provider' or 'contractor.'"

This means that even where a nonprofit organization is not covered as a business, its service provider may nonetheless have responsibilities under the CPRA.

Second, in what may be a significant relief to many service providers, the draft regulations explicitly allow service providers to use personal information obtained from one customer to improve a product or service for all customers, provided the personal information is not "used to perform services on behalf of another," such as by marketing to the business's customers on behalf of another company.

As this sort of internal use is often critical for service providers — and without the explicit exception, arguments could be made that such a use is a hallmark of a sale of personal information to the vendor — this is a key provision for businesses and service providers alike.

Third, the draft regulations provide a checklist of the CPRA's requirements for third-party agreements, which can assist businesses in revising their vendor contracts and templates in anticipation of the CPRA.

Third Parties

The draft regulations impose obligations on nonvendor third parties also.

Significantly, even a business that sells or shares personal information must enter into an agreement with the third-party recipient of the personal information that includes requirements substantially similar to those in service provider contracts, such as requiring the third party to only use and retain the personal information for the narrow purposes for which the personal information is being sold or disclosed, and to comply with the CPRA.

In addition, the draft regulations imply a requirement to perform adequate due diligence (or else face diminished ability to blame the third party), which encourages businesses to ensure their due diligence processes are sufficient.

Notifications Regarding Third-Party Data Collection

The draft regulations add a new concept requiring the notification of third-party involvement in the collection of personal information.

If another party is involved in and controls collection of information — e.g., a cookies analytics provider — then the business must inform consumers about that collection and the third party.

As a more concrete example, the draft regulations state that if a coffee shop allows a business providing Wi-Fi to collect personal information, then the coffee shop must inform customers of that third-party data collection through a sign or other signals.

Limits on Use of Sensitive Personal Information

The draft regulations operationalize the new right to limit the use of sensitive personal information under the CPRA, most notably providing a list of exceptions when businesses may use or disclose sensitive personal information without being required to offer consumers a right to limit such uses or disclosures.

The list of exceptions includes circumstances when the information is necessary to:

- Perform services or provide goods, as reasonably expected by an average consumer who requests those goods or services;
- Detect security incidents to resist malicious or illegal attacks on the business;
- Ensure the physical safety of natural persons;
- Short-term, transient use;
- Perform services on behalf of the business; or
- Verify or maintain the quality or safety of the business.

Consumer Requests to Correct Information

The draft regulations also operationalize the new right recognized under the CPRA to correct inaccurate personal information, requiring businesses to take a multistep analysis, including reviewing the totality

of the circumstances, such as the nature of the information, how it was obtained, and documentation relating to the accuracy of the information.

At the business's choice, a business may delete the information if such deletion does not negatively affect the consumer or the consumer consents to the deletion.

The relevant section of the draft regulations also provides specific examples relating to data brokers, and requires that where a business is not the source of the inaccurate information, the business must disclose the name of the source supplying the inaccurate information.

Opt-Out Preference Signals

The draft regulations add a definition for opt-out preference signal, which is a signal sent by a platform, technology or mechanism on behalf of the consumer that communicates the consumer's choice to opt out of the sale and sharing of personal information.

Notably, the draft regulations require businesses to process all consumer opt-out preference signals that meet certain requirements. Under the draft regulations, when a business detects an opt-out signal, it must treat it as a bona fide opt-out request, process these opt-out signals in a frictionless manner, and indicate to consumers that they have opted out of the sale of their personal information.

Interestingly, the draft regulations indicate that a self-serve cookie management control process alone would not be sufficient to effectuate requests to opt out of sales and/or sharing, because "cookies concern the collection of personal information and not the sale or sharing of personal information."

Such signals have been a source of ongoing confusion for businesses. While the draft regulations provide additional clarification, technical questions remain as to how these signals may or may not be communicated to a business, and what choices businesses have to present opt-outs and links, or otherwise to ensure they effectively respond to consumers' opt-out signals.

Data Minimization and Retention

The draft regulations include a section on the CPRA's data minimization requirement, which asks that businesses to collect, use, retain and/or share consumers' personal information according to "what an average consumer would expect."

Any collection, use, retention or sharing that does not meet this standard requires additional notice and the consumer's explicit consent — subject to the dark patterns analysis above — and the regulations provide examples to help illustrate these requirements.

This new requirement drastically changes permissible practices with respect to consumer data, and provides a hook for the agency to find impermissible processing of information, a concept that was largely missing from the California Consumer Privacy Act.

Significant Definitions

The draft regulations propose numerous additions and changes to the definitions provided in the original California Consumer Privacy Act draft regulations, some of which grapple with the daunting realities faced by businesses attempting to comply with consumers' requests.

For example, under the proposed regulations, businesses would be able to tailor their compliance to take into account overly burdensome or unreasonable requests based on the nature of the data at issue — e.g., large video files that are both cumbersome to access and difficult to search, as part of the newly defined "unstructured data," which does not have a defined internal structure — and the burden that complying with such a request would place on the business, newly defined "disproportionate effort."

These additions take a step toward balancing consumers' legitimate rights and interests with the practical realities faced by businesses.

What Is Not Addressed by the Draft Regulations

One of the most conspicuous omissions from the draft regulations concerns the lack of parameters for automated decision making. The CPRA defines "profiling" as "any form of automated processing of personal information, as further defined by regulations," leaving the contours relatively amorphous in scope.

The CPRA's language casts a wide net that could be argued to cover everything from facial recognition in public places to automated processes like calculators and spellcheckers that may process personal information.

As expressed in many agency public record comments, numerous stakeholders hoped the initial set of regulations would clarify this definition, for example, by limiting it to automated technologies that could create a material impact on a person. That task was punted in the current draft regulations, with an unknown timeline, leaving many in limbo.

Another significant omission concerns the CPRA's requirement for businesses to conduct annual cybersecurity audits and risk assessments if their "processing of consumers' personal information presents significant risk to consumers' privacy or security."

The draft regulations do not provide further specificity around these requirements. Businesses will have to wait to see more about what steps are required as part of these assessments, and whether they are covered in the first instance.

Conclusion

These draft regulations are a key milestone for the agency's rulemaking. Nonetheless, significant details remain outstanding, and the regulations are likely to change as the rulemaking process continues.

In the meantime, given the proximity to the effective date, companies may wish to consider undertaking additional compliance steps guided by the agency's draft regulations, including:

- Reviewing consent flows and cookie banners for dark patterns;
- Supplementing third-party data sharing agreements to enhance privacy and security protection;
- Considering how and when to notify users regarding joint entity data collection points; and
- Ensuring that each category of data collected is reasonably targeted to the business's product and service offerings, including through data mapping.

Cassandra Gaedt-Sheckter is a partner at Gibson Dunn & Crutcher LLP.

Alexander Southwell is a partner at the firm and co-chairs the firm's privacy, cybersecurity and data innovation practice group. Southwell previously served as an assistant U.S. attorney in the Southern District of New York.

Ryan Bergsieker is a partner at the firm.