CPRA Rulemaking Is Underway —Getting Ahead of Enforcement Risks

August 2, 2022

On July 8, 2022, the California Privacy Protection Agency (the "Agency") issued a Notice of Proposed Rulemaking, kicking off a forty-five day comment period for proposed updates to the California Consumer Privacy Act ("CCPA") regulations. These updates streamline the CCPA regulations and revise them to reflect the changes made by the amendments in the Consumer Privacy Rights Act of 2020 (the "CPRA"). Even if they are substantially modified before becoming final, the proposed regulations shed light on the Agency's approach to consumer protection, which appears focused on: (1) user experience and ease of exercising rights; (2) purpose limitation of data collection; and (3) transparency around third-party data collection.

This post is the first in a planned series of blog posts addressing the CCPA rulemaking and key issues reverberating from the stakeholder and informational sessions, as well as important updates from the notice and comment period.

The proposed regulations will have wide-ranging operational and governance implications for many companies. In addition to proposed changes to how businesses should operationalize consumer rights enshrined by the CPRA, key provisions in the proposed regulations include:

User Experience. The proposed regulations outline how businesses should operationalize CCPA data-subject requests from consumers and, where required, obtain consumer consent. The proposed regulations emphasize simplicity, ease of use, and symmetry in choice, and provide detailed guidance on activities that the Agency considers "dark patterns" that have the effect of nullifying consumer choice. Examples include bundling consent to the use of personal information ("PI") for reasonably expected purposes together with other secondary purposes and a website banner that only allows consumers to "accept all" but not "decline all" cookies.

Purpose Limitation and Consent. The CPRA provides that a business's processing of PI must be reasonably necessary and proportionate to achieve the purposes for which it was collected and that a business cannot use consumer PI that was initially collected for one purpose for a different, unrelated purpose. The proposed regulations expand this by

defining what is "reasonably necessary and proportionate" to be consistent with consumers' expectations and require businesses to obtain explicit consent before "collecting, using, retaining, and/or sharing the consumer's [PI] for any purpose that is unrelated or incompatible with the purpose(s) for which the [PI] [is] collected or processed." The proposed regulations provide numerous examples of when consent is required. For example, a cloud storage company can use consumer-provided PI to improve their services for said consumer but cannot use the PI to research and develop unrelated or unexpected products without first obtaining explicit consent from the consumer.

Businesses must ensure that consumers can understand and easily decline consent requests and also avoid manipulative language or choice architecture such as bundling consent for incompatible uses. If the consent method fails to meet these requirements, it may be considered a "dark pattern," thereby vitiating any "consent" provided.

Detailed Requirements for Service Providers, Contractors, and Third Parties.

The CPRA defines three types of entities with whom a business that is subject to the CCPA may, pursuant to a written contract, disclose data: Service Providers, Contractors, and Third Parties. Service Providers are entities that process consumer information for a business purpose. Contractors are those entities to whom the covered business "makes available a consumer's personal information for a business purpose." A Third Party is any person who is not a regulated business, Service Provider, or Contractor.

The proposed regulations emphasize that contracts with all entities must:

- identify and define the "specific business purpose(s) and services(s)" for which the data will be provided, processed, sold, or disclosed;
- require entities to notify covered businesses within five business days if the entity cannot meet its CCPA obligations;
- require entities to "take reasonable and appropriate" steps internally, upon notice, to "stop and remediate" any unauthorized data use; and
- require entities to comply with consumer rights requests to opt out of the sale of or for the deletion of data made to the business upon notification by the business.

The proposed regulations also indicate that businesses must enforce contractual provisions or exercise their contractual rights to perform due diligence on service providers, contractors, and third parties. More specifically, "a business that never enforces the terms of the [entity] contract" (and, in the case of Service Providers and

Contractors, never "exercises its rights to audit or test the service provider's or contractor's systems") "might not be able to rely on the defense that it did not have reason to believe that the [entity] intends to use the [PI] in violation of the CCPA."

Irrespective of contractual requirements, all Service Providers, Contractors, and Third Parties must also "comply with all applicable sections of the CCPA and these regulations, including providing the same level of privacy protection as required by businesses" and "implementing reasonable security procedures and practices appropriate to the nature of the personal information received" from the business. Such compliance can consist of Service Providers and Contractors cooperating with consumer requests made pursuant to the CCPA and adopting reasonable security measures, and Third Parties taking a number of actions, including "only collecting and using [PI] for purposes an average consumer would reasonably expect[.]"

Third-Party Notices. The Agency clarified the Notice-at-Collection requirements, with a focus on data collection by third parties. A first-party business—that is, "the consumer-facing business with which the consumer intends and expects to interact"—must name or describe the business practices of any third parties that control PI collection on the first-party business's website or premises. The third party must also give a clear Notice at Collection. If a consumer requests to opt out of sale/sharing with the first party, both the first party and third party(s) that control the data collection sshall process and comply with the consumer's request and forward the request to other third parties that might have access to said data.

Investigation and Enforcement Process. The proposed regulations outline four investigation and enforcement tools at the Agency's disposal: (i) consumer complaints (which can be sworn or anonymous); (ii) Agency audits; (iii) stipulated orders with the Head of Enforcement; and (iv) probable cause proceedings with the Enforcement Division. The Agency may conduct an audit to investigate possible violations of the CCPA, and alternatively, the Agency may conduct an audit if the subject's collection or processing of personal information presents a significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law. While the Agency has yet to hire any Enforcement Division staff, the robust enforcement framework outlined in the regulations suggests that the Agency is eager to commence enforcement as soon as possible.

Key areas where the Agency must create regulations, but are not addressed in these regulations, include:

Automated Decision-Making ("ADM"). Future regulations will address access and opt-out rights associated with businesses' ADM use, including "profiling and requiring 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."

Risk Assessments. Under the CPRA, businesses that process consumer PI that presents a significant risk to consumers' privacy or security must submit risk assessments to the Agency "on a regular basis." Risk assessments should identify and weigh the benefits of processing consumer PI against potential risks to the consumer.

Cybersecurity Audits. The CPRA requires businesses that process consumer PI that presents a significant risk to consumers' privacy or security to undergo annual cybersecurity audits. Future regulations will address the scope of said audits and ways to ensure that they are thorough and independent.

The Agency has already held stakeholder sessions on these topics and noted in their Notice of Proposed Rulemaking that these topics would be the subject of future rulemaking.

KEY TAKEAWAYS

With all this in mind, there are a number of steps that companies can consider in order to reduce enforcement risk.

Start Now. Companies should start considering how the proposed regulations could impact business plans and in-flight projects. Businesses should identify which processes might take the longest to implement and prioritize starting on those.

Map and Track Data. The proposed regulations underscore the value of having a holistic understanding of how and where PI is collected and where that data is transferred, sold, or shared. This will allow companies to more effectively communicate consumer requests to opt out, correct, or delete—as well as denied requests to correct—to outside entities. Additionally, companies armed with this knowledge will have a better understanding of whether they can effectuate a consumer request to correct in the first place, and if not, why.

Evaluate Purposes for Processing and Mechanisms for Consent. Another potential area for enforcement focuses on when and how companies obtain consumer consent in circumstances where the data will be used for an incompatible purpose. Legal departments should consider working closely with product teams, especially those that use consumer PI, to identify potential uses of the PI and consider whether the consumer PI usage is "unrelated" or "unexpected" such that explicit consumer consent is necessary.

The consent should be easy to understand and execute, provide "[s]ymmetry in choice" (i.e., selecting a "more privacy-protective option" should not be more onerous than selecting a "less privacy-protective option"), and avoid confusing or manipulative language or architecture. If the California Attorney General's 2021 enforcement examples are any predictor, it is likely that the Agency and Attorney General will expect that covered companies get the basics right, making these notices and mechanics easy targets for enforcement.

Update Written Procedures. Documenting procedures is crucial from both compliance and enforcement perspectives. Business should take a look at existing policies with an eye to addressing: (i) how to effectuate consumer data requests; (ii) when to obtain affirmative consent from consumers; (iii) how to provide opt-out notices; and (iv) how to manage Service Providers, Contractors, and Third Parties to adhere to these new regulations. The Attorney General's prior enforcement examples suggest leniency in enforcement where good-faith efforts at compliance are made but have fallen short.

Revise Contracts. The proposed regulations will require careful review and likely revision of preexisting contracts involving data transfers. Companies should identify contractual arrangements involving the disclosure of personal data and draft addenda that clearly articulate the nature of the relationship between the parties and align with the regulatory standards. Businesses can further mitigate regulatory risks by considering and documenting how consumer requests that implicate more than one Service Provider, Contractor, or Third Party will be handled so that all parties can meet their obligations.

Integrate with Vendor Diligence and Risk Management. The proposed regulations place particular weight on covered companies' knowledge and management of Service Providers, Contractors, and Third Parties that hold PI. As discussed above, a business that does not exercise its contract enforcement rights "might not be able to rely on the defense that it did not have reason to believe that the [entity] intends to use the [PI] in violation of the CCPA." Companies should therefore consider updating their vendor-risk management programs to include regular reviews of vendors and other parties that hold their consumer PI in order to evaluate compliance with contractual requirements and the CCPA.

To subscribe to the Data Blog, please click here.

The authors would like to thank Debevoise Law Clerk Elise Coletta and Summer Associate Peg Schreiner for their work on this Debevoise Data Blog.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

Michael R. Roberts
mrroberts@debevoise.com

SAN FRANCISCO

David Sarratt
dsarratt@debevoise.com

Christopher S. Ford
csford@debevoise.com

H Jacqueline Brehmer
hjbrehmer@debevoise.com