New California Draft Privacy Regulations: How They Would Change Business Obligations and Enforcement Risk

Alysa Z. Hutnik, Aaron J. Burstein, Laura Riposo VanDruff, Alexander I. Schneider

May 30, 2022

On Friday May 27, 2022, the California Privacy Protection Agency (CPPA) Board announced its next public meeting will be on June 8, 2022. The announcement simply stated the date of the meeting, that there are "some discussion items [that] will be relevant to the Agency's rulemaking work," and that information on how to attend the meeting and the meeting agenda could be found on the CPPA's site. It did not take too many Internet sleuths to review the posted agenda, and note that Agenda Item No. 3 was "*Discussion and Possible Action Regarding Proposed Regulations, Sections 7000–7304, to Implement, Interpret, and Make Specific the California Consumer Privacy Act of 2018, as Amended by the California Privacy Rights Act of 2020, Including Possible Notice of Proposed Action*," and that the posted meeting materials included a copy of the "Draft Proposed CCPA Regulations." In addition, Agenda Item No. 4 provides for "Delegation of Authority to the Executive Director for Rulemaking Functions." Full stop, June will be an active month for California privacy rulemaking.

But let's unpack the surprises in the draft regulations. The 66-page draft proposed CCPA regulations (and they are referred to within the document as CCPA regulations) take a prescriptive approach to privacy obligations. In concept, that is not too surprising. Of concern, in some areas, they uniquely depart from approaches set forth by other state privacy laws. The quiet release of dramatic new obligations while bipartisan Senators reportedly may be reaching consensus on federal privacy legislation that could preempt state law obligations puts companies doing business in California in a difficult position. Do they scramble to operationalize new programs to comply with the CPPA's new requirements, if finalized? Do they wait on Congress? Do they choose a third path? For now, while these draft rules are certain to change in some respects before they are finalized, they directionally outline a new privacy baseline for the United States. We highlight certain aspects of the draft rules below, with a particular focus on accountability and risk exposure, how data can be shared with other businesses for digital advertising or other functions, and what those business agreements must include to lawfully support such business relationships and comply with the amended CCPA.

Quick and Costly Potential CPPA Enforcement

Consumers, the CPPA, and the California Attorney General's Office all are empowered to take businesses (and contractors, service providers, and third parties) to task for perceived non-compliance with privacy obligations. Among all of the proposed changes in the draft regulations, the enforcement provisions should cause many companies, regardless of their role, to pause and

evaluate whether they've allocated sufficient resources to address privacy compliance. While there is not a privacy private right of action under the CCPA/CPRA, the draft rules set forth a new increased, and fast tracked form of compliance monitoring and action that could be surprising to many companies and costly.

First, while there are provisions about requiring consumers to file sworn complaints, the CPPA provides that it can accept and initiate investigations on unsworn and anonymous complaints too. For every sworn complaint, the CPPA must notify the consumer complainant in writing of what actions the Agency has taken or plans to take and the reasons for action or non-action. Because the Agency has to respond to each complaint, this could turn into a routinized process of a high volume of complaints forwarded to businesses, with tight timeframes to respond in writing or else face violations and administrative fines.

The rules provide that there is "probable cause" of a privacy violation if "the evidence supports a reasonable belief that the CCPA has been violated." There is no mention of extensions of time for good faith reasons. Under the statute, the CPPA can find a violation through a probable cause hearing if it provides notice by service of process or registered mail with return receipt to the company "at least 30 days prior to the Agency's consideration of the alleged violation." The notice must contain a summary of the evidence, inform the company of their right to be present "in person and represented by counsel." The "notice" clock starts as of the date of service, the date the registered mail receipt is signed, or if the registered mail receipt is not signed, the date returned by the post office. It's possible this process occurs through the forwarding of unverified consumer complaints.

Under the draft rules, a company can request the proceeding be made public if they make a written request at least 10 business days before the proceeding. A company has a right to an in-person proceeding only if it requests the proceeding be made public. Otherwise, the proceeding may be conducted in whole or in part by telephone or video closed to the public. Participants are limited to the company representative, legal counsel, and CPPA enforcement staff. The CPPA serves as prosecutor and arbiter, and the draft rules do not define how the agency preserves its neutrality in its latter role.

The CPPA makes a determination of probable cause at such proceeding "based on the probable cause notice and any information or arguments presented at the probable cause proceeding by the parties." If a company does not participate or appear, it waives "the right to further probable cause proceedings" (it's not clear in the draft rules whether that is limited to the facts of that matter, or future alleged violations) and a decision can be made on the information provided to the CPPA (such as through a complainant).

The CPPA then issues a written decision and notifies the company electronically or by mail. Of concern, the draft rules provide that this determination "is final and not subject to appeal." Under the statute, violations can result in an administrative fine of up to $2500 for each violation, and up to $7500 for each intentional violation or if the violation involves minors. Multiple parties involved can be held jointly and severally liable. It's conceivable that violations may be calculated on any number of factors that could add up substantially, and as contemplated by these draft rules, there is no process to challenge such judgments, including if there are factual or legal disputes. One can imagine future legal proceedings that challenge a variety of the legal bases for such a structure if these rules are finalized as drafted.

Service Provider Requirements and Restrictions

Data Privacy Addendums Get a Further Tune Up, and Open Question on Whether They Need to be Bespoke. One aspect of state privacy law compliance that has consumed much resources and time are the service provider contracts. Who is a service provider? What must the contract say? What restrictions apply to service providers (or contractors)? The draft rules continue to add more obligations.

One must have a written contract in place that meets all of the requirements outlined below to even qualify as a service provider and contractor. The contract requirements are very granular, and go beyond what most current privacy addendums (or technology provider terms and conditions) look like today, and include:

- Restrictions from selling or sharing the business's personal information.
- Identify which specific business purposes and services are required for processing the business's personal information, and that such disclosure occurs only for the limited and specified business purposes set forth in the contract. This cannot be stated generally with reference to the agreement, but rather requires a specific description.
    - *This language suggests that a one-size-fits-all data processing agreement for all vendors processing personal information for different business purposes or functions might not be sufficient, which is very concerning from a resource and practicality standpoint*.
- Restricting the processing of personal information outside or for any other purpose from those business purposes in the contract, including to service a different business, unless permitted by the CCPA. Awkwardly, the proposed rule suggests that all of the specific business purpose(s) and service(s) identified earlier would need to be restated as part of the restrictions.
    - *On this last point, the draft rules underscore this specific example: "a service provider or contractor shall be* ***prohibited from combining or updating*** *personal information received from, or on behalf of, the business with personal information that it* ***received from another source*** *unless expressly permitted by the CCPA or these regulations*"
- Requiring compliance with all applicable provisions of the CCPA, including providing the same level of privacy protection as applicable to businesses, to cooperate with the business for handling consumer rights requests, and reasonable data security provisions.
- Reasonable audit provisions to ensure CCPA compliance, such as "ongoing manual reviews and automated scans of the service provider's system and regular assessments, audits, or other technical and operational testing at least once every 12 months."
- Notification to the business within 5 business days if the service provider/contractor determines it cannot meet its obligations.
- Providing the business the right to take reasonable steps to stop and remediate any unauthorized use of personal information by the service provider/contractor, such as "to provide documentation that verifies that [the service provider/contractor] no longer retain[s] or use[s] the personal information of consumers that have made a valid request to delete with the business."
- Provides that the business will notify the service provider/contractor of any consumer rights request and provide the information necessary for the service provider/contractor to comply with the request.

In addition to the contract, the draft rules emphasize that these cannot just be words on paper that diverge from actual practices. Section 7051(e) notes in particular that, in assessing compliance, the CPPA can evaluate whether the business conducted any due diligence to support a reasonable belief of privacy compliance, and whether and how the business enforces its contract terms, including performing audits. If there is non-compliance, both parties can be held jointly and severally liable.

The Limitations on Internal Use of Customer Data by a Service Provider/Contractor. The draft rules provide that a service provider/contractor is restricted from using customer personal data for its own purposes, except for internal use to build or improve the quality of its services, provided that the service provider/contractor does not use the personal information to perform services on behalf of another person in a manner not permitted under the CCPA. This language is notably different from the governing CCPA rules. Based on the examples outlined below, and the admonition above that the service provider cannot combine or update personal information received from another source unless permitted by the CCPA, makes it ambiguous as to when updating personal information crosses the line. From the examples, it suggests that where such functions are to facilitate personalized advertising or data sales, they would not fit within a service provider/contractor role.

Use for Analysis/Data Hygiene (Sometimes). The draft rules set forth two examples that seem to allow some analysis and data correction under particular circumstances. For example, the first illustration emphasizes that the service provider/contractor can analyze how a business customer's consumers interact with company communications to improve overall services, and the second example highlighted that a service provider/contractor can use customer data to identify and fix incorrect personal information that, as a result, would improve services to others. The draft rules underscore, however, that a service provider/contractor could not compile (e.g., enrich/append) personal information for the purpose of sending advertising to another business or to sell such personal information.

Data Security/Fraud Prevention. Consistent with the statute, the draft rules allow service providers/contractors to use and combine customer personal information "[t]o detect data security incidents or protect against malicious, deceptive, fraudulent or illegal activity."

Other Legal Purposes. The draft rules acknowledge that a service provider/contractor can use customer data to comply with other laws, lawful process, to defend claims, if the data is deidentified or aggregated, or does not include California personal information.

Advertising Service Provider Functions Look Limited. The draft rules acknowledge a business can engage a service provider/contractor for advertising/marketing services if the services do not combine opted out consumer data from other sources. The draft rules also affirmatively reiterate that an entity who provides cross-contextual behavioral advertising is a third party and not a service provider/contractor.

- As an example of what would cross the line, the draft rules provide that a service provider/contractor can provide non-personalized advertising based on aggregated or demographic information (ads based on gender, age range, or general geographic location), but could not, for example, share the business's customer information with a social media platform to "identify users on the social media company's platform to serve advertisements to them." This example is stated without qualification to what commitments the platform has provided on its own use and restrictions as to such data, or if and how any other permitted "business purposes" under the CPRA may apply.
- In another example, the draft rules provide that an advertising agency can be a service

provider/contractor by providing contextual advertising services. Again, this example is set forth without reference to any other business purposes that may apply. However, one wonders whether the enforcement structure may inhibit broader interpretations where functions involve personalized advertising and analytics.

Third Parties that "Control the Collection" of Personal Information

Notice at Collection. The draft rules have new language that, in the context of "notice at collection" provide that when more than one party controls personal information collection, such as in connection with digital advertising, all such parties must provide a very detailed "notice at collection" that accounts for all parties' business practices. As an example:

- A "first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a notice at collection."

Both parties also would need to honor opt outs of sale/sharing, and the "notice at collection" would need to include "**the names of all the third parties** that the first party allows to collect personal information from the consumer," or the first party can include in its "notice at collection" the information provided by the third party that would meet all of the requirements about its business practices. For example, a company that has a third party analytics tag on its website would need to post a conspicuous link to its "notice at collection" about the analytics company's information practices on its homepage and all webpages that include the tag collecting personal information. The analytics company also would need to post a "notice at collection" on its website's homepage. These requirements also apply offline, where applicable.

Honoring Opt Outs. Section 7051 provides that third parties are directly obligated to honor opt outs, including as conveyed through a global privacy signal or otherwise on a first-party business's site hosting the third party's tag collecting personal information, unless the first-party business informs the third party that the consumer has consented to the sale/sharing, or "the third party becomes a service provider or contractor that complies with the CCPA and these regulations."

- *This latter provision is interesting because it suggests implicit support for frameworks, such as IAB's LSPA, where a contract that contains commitments around use of personal data post-opt outs can support a continued service provider role.*

The first-party business would also be required to "contractually require the third party to check for and comply with a consumer's opt-out preference signal unless informed by the business that the consumer has consented to the sale or sharing of their personal information. A contract must be in place with the first party in order for the third party to lawfully collect and use personal information collected from the first party site by a third party. The contract would need to comply with all of the express requirements for such third party contracts under the CCPA. As with service providers/contractors, these contract provisions are very detailed, and due diligence and accountability provisions are also required.

* * *

There is a lot to consider and while all of these provisions remain subject to further changes, it is clear that the draft rules suggest a more exacting expectation as to privacy compliance by companies doing business in California or otherwise with California residents, and an expansive new

set of obligations to tighten such compliance within the information supply chain. We will cover in future blog posts how these draft rules contemplate other business obligations, including as to obligations around obtaining consent, privacy policies, responses to consumer privacy rights, the use of sensitive personal information, and mechanics of complying with opt out of sales/shares, and global privacy controls. If you are interested in submitting comments in the rulemaking process or have questions about privacy compliance, please reach out to members of Kelley Drye's privacy team.

JOIN US

Separately, join us as Kelley Drye privacy lawyers provide observations on the proposed regulations, including which would pose the biggest challenge for businesses if implemented, and will offer strategies to plan efficiently for compliance in the face of these proposals. **Register here**.