The Employment, Compliance & Privacy Report

Beckstead Terry PLLC

CCPA Update: Preparing for the CPRA Amendments Despite Regulatory Delays

By Jana Terry, March 4, 2022

The California Consumer Privacy Act (the CCPA) was amended last year by the California Privacy Rights Act (the CPRA). Businesses subject to these California privacy laws must be compliant with the CPRA by January 1, 2023. Enforcement of the CPRA will begin on July 1, 2023.

Final Regulations Delayed

Knowing how difficult it was for businesses to come into compliance with the original CCPA in the absence of regulatory guidance, the drafters of the CPRA included a statutory requirement that the newly-created and first-of-its-kind California Privacy Protection Agency promulgate final regulations by July 1, 2022. That way, businesses would have a full six months in which to operationalize compliance, before the CPRA went into effect. Despite the statute's requirement, the Agency recently made it clear that it will not meet the July 1, 2022 deadline. Instead, Ashkan Soltani, the Agency's executive director, announced that regulations will not be finalized until the 3rd or 4th quarter of 2022.[1]

This delay means that companies face a compliance deadline of January 1, 2023, without the promised six-month window of time in which to understand and operationalize the regulations. This presents a significant challenge because the scope of Agency rulemaking is going to be extensive, compared to the regulatory effort required for implementation of the original CCPA.

Expected Scope of Regulations

The CPRA requires the Agency to provide regulations on more than 20 topics. For some of the topics, it will be difficult for companies to comply with the CPRA prior to the required rulemaking. For example, among other things, the Agency is supposed to provide additional and clarifying definitions and issue new regulations pertaining to opt-out signals, sensitive PI, requests to correct PI, and the obligation to conduct audits and submit risk assessments. These are some of the Agency tasks that will not be finalized by the July 1, 2022 deadline:

- Rules and procedures for (a) consumer opt-outs from "sharing" of PI and (b) consumer requests to limit the use of sensitive PI
- Technical specifications for "opt-out preference signals" that must be honored by businesses
- Regulations on how businesses can provide subsequent opportunities for opt-in
- Technical specifications for opt-out preference signals for minors

- Regulations on access and opt-out rights with respect to automated decision-making technology
- Clarification about when a business's processing of PI "presents significant risk to consumers' privacy or security" such that audits and risk assessments are required
- The nature and scope of any required cybersecurity audits and risk assessments
- Regulations on businesses' use and disclosure of consumers' sensitive PI
- Regulations regarding the circumstances under which sensitive PI is collected or processed "without the purpose of inferring characteristics about a consumer" such that it should be treated as ordinary PI (rather than sensitive PI)
- Rules about when a business has to comply with a request to correct PI (including how the business may respond, steps the business may take to prevent fraud, and the extent to which a consumer may have the right to provide an addendum)
- Exceptions to protect trade secrets and intellectual property
- Regulations on when it is "impossible" or would require "disproportionate effort" for a business provide information beyond a 12-month period
- Explanation of (i) the "business purposes" for which a business, service provider and contractor may use PI, (ii) when service providers and contractors may combine consumers' PI obtained from different sources, and (iii) when service providers and contractors may use the PI they receive for their own business purposes
- Definitions regarding—
    a. when a consumer "intentionally interacts" with a business, app, website or service (for purposes of determining whether a consumer is being targeted with "cross-context behavioral advertising"),
    b. the meaning of "precise geolocation," especially in the context of sparsely populated areas and as distinct from the information used by businesses for normal operations such as billing,
    c. "dark patterns" and "deidentification" of data,
    d. "specific pieces of information,"
    e. what constitutes a "law enforcement agency-approved investigation" for purposes of a business's obligation not to comply with a consumer request to delete.[2]

There is no question that the above topics cover *a lot* of ground. But given the delayed regulatory timeframe, it is no longer a reasonable strategy to wait for the regulations to become final before starting to work toward CPRA compliance CPRA.

"Top Ten" ways to prepare for CPRA compliance before the regulations are final

While we are waiting for regulatory guidance on the topics above, companies would do well to get started on everything else. And notably, there are several significant changes required by the CPRA that are *not* on the above list of regulatory tasks—and, therefore, there is no reason to wait.

Over the next few months, this blog will cover these top ten ways that companies can prepare for the CPRA even before the regulations become final:

1. Prepare for the CPRA's elimination of the 30-day "right to cure" by making sure you understand how the Attorney General has been interpreting and enforcing the CCPA.
2. Prepare for an expansion of the CPRA private right of action.
3. Determine whether and how you collect and process "sensitive PI."
4. Prepare to apply the CCPA to your California employees.
5. Prepare to apply the CCPA to your business-to-business contacts.
6. Examine whether your financial incentive programs comply with the current regulations (as interpreted by the AG) and prepare to operationalize the 12-month waiting period that will apply before you can "re-ask" a consumer to opt-in.
7. Understand how your company uses ad tech so you will be able to disclose whether and how your company "shares" PI for cross-context behavioral advertising.
8. Prepare for the likelihood that your company will have to provide an "opt-out" option for "selling" or "sharing" PI.
9. Incorporate GDPR-like data minimization and proportionality principles into your privacy policies.
10. Prepare to disclose your data retention policies (or how you will make data retention decisions in the absence of specified policies).

As this "top ten" list shows, there is plenty of work that can be accomplished before the Agency releases its final regulations in late 2022. Stay tuned for more information on getting started.

---

[1] Joseph Duball, *CPRA Regulations Delayed Past July 1 Deadline, Expected Q3 or Q4,* IAPP Privacy Advisor, Feb. 23, 2022, https://iapp.org/news/a/cpra-regulations-delayed-past-july-1-deadline-expected-q3-or-q4/.

[2] Most of the items on this task list are found in CCPA Section 1798.185, the "Regulations" section of the CCPA (as amended by the CPRA). A copy of the current CCPA (with the CPRA amendments redlined against the original CCPA) can be found at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf