LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice

October 22, 2019 | Number 2550

California Consumer Privacy Act Draft Regulations: What's New, What's Next

Covered businesses have much work to do to revise disclosures, implement choice mechanisms, and design compliant data subject request programs.

Key Points:

- The Attorney General's draft regulations, released on October 10, 2019, will be available for public comment until December 6, 2019, after which they will likely undergo some further revisions before becoming enforceable on July 1, 2020.
- Violations of the CCPA between its January 1, 2020, effective date and the regulations' July 1, 2020, enforcement date remain a risk, so waiting for the final rules is not a viable compliance plan.
- The Attorney General's fact sheet announcing the regulations warned that compliance with the GDPR will not constitute a de facto or actual "safe harbor" for demonstrating compliance with the CCPA — the laws are too different for such an approach.
- Under key draft regulations, covered businesses must:
  - Describe in their privacy policy the specific process by which they will verify consumer requests.
  - Implement technical or other effective means to recognize and respond to "user-enabled privacy controls" (such as Do Not Track signals, signals sent by browser plug-ins, and privacy settings) as valid affirmative requests to opt out — if such businesses "sell" personal information
  - Respond to data rights requests from non-account holders even if verification is not certain so long as the requestor's identity can be verified to a "reasonable" or "reasonably high" degree of certainty
  - Respond to requests for access or deletion even if the requests were submitted through improper means — if verified, such requests must be fulfilled or responded to with instructions on proper submission
  - Treat unverified requests for deletion as valid requests for opt-out and treat unverified requests for specific pieces of information as valid requests for categories of information collected
  - Compile and disclose metrics on data requests/responses — if such businesses handle large volumes of consumer personal information (4 million consumers minimum)
  - Maintain records of data rights requests and responses for 24 months
  - Notify consumers and obtain their explicit consent to any new use of previously collected personal information (codifying long-standing FTC guidance)

CCPA Basics

The California Consumer Privacy Act (CCPA) is now final — Governor Gavin Newsom signed the key amendments into law on October 11, 2019 — and will take effect on January 1, 2020.

The CCPA applies to companies doing business with and collecting personal information from California consumers (subject to certain threshold parameters). Among other things, the CCPA provides consumers with the following rights over their personal information: (i) the right to know the categories of personal information a business has collected about them, how it is used, and how it is sold or shared; (ii) the right to know the specific pieces of personal information collected or maintained about them; (iii) a (highly qualified) right to request the deletion of personal information; (iv) the right to opt out of the sale of their personal information; and (v) the right to not be discriminated against for exercising these aforementioned rights. The law also imposes transparency obligations that require covered businesses to disclose what information they collect, how it is used, how it is shared, as well as provide notice of available data rights.

The CCPA provides consumers a private right of action against a covered business for a data breach resulting from the business's breach of its "duty to implement and maintain reasonable security procedures and practices." The CCPA, however, does not provide a private right of action for any other violation of its other provisions.

Attorney General Enforcement Authority

The Attorney General (AG) has significant enforcement authority to allege violation(s) of the CCPA against any covered business. The allegation triggers a 30-day period in which the business may cure the violation(s). If the covered business fails to cure, the AG may bring a civil action for the violation(s), which could result in an injunction and potential penalties of US$2,500 per violation and US$7,500 per intentional violation. Penalties for non-compliance calculated per violation could quickly reach substantial levels, especially for businesses with extensive amounts of personal information from many consumers.

The draft regulations add specificity to this enforcement authority. While regulations might seem more suggestive than authoritative, under California law, when a statute designates a state agency with rulemaking authority, the regulations promulgated under that authority have the force of law. In other words, the final regulations here will have equal legal force as the statutory text of the CCPA itself. Violations of the final regulations could trigger the same regulatory scrutiny and penalties as violations of the underlying statute.

Once the draft regulations are formally codified, they will be subject to judicial review. In past cases, the California Supreme Court has stated that it will declare regulations void when they fail to "conform to the legislative will" or "violate acts of the Legislature."[1] Regulations may also face scrutiny where an agency has made a "fundamental policy determination," such as undoing "a clearly established legislative priority."[2] Thus, challengers of these regulations may question to what extent they deviate from the underlying legislative will vis-à-vis the CCPA itself.

Regulations Explained

Consistent with the broad statutory mandate to the AG to implement the law through detailed regulations, the draft regulations propose to augment the CCPA with new substantive requirements, and in general, to create significant new compliance burdens for covered businesses. Many aspects of the law require company-specific legal and occasionally economic analysis, which will be non-trivial and essential for companies to get right. Many commentators predict a widespread lack of material compliance, certainly as of the January 2020 effective date (when the final regulations will not even be out). Setting aside the

chaotic legislative and rulemaking process, covered businesses should not delay coming into a defensibly compliant posture with the law, as informed by these draft regulations.

Data Rights Requests

Covered businesses must recognize and treat consumers' use of technical privacy controls as valid requests to opt out. Covered businesses must now treat "user-enabled privacy controls," such as browser plug-ins, privacy settings, Do Not Track requests, or "other mechanism," as valid requests to opt out for that browser or device, or, if known, for the consumer setting the controls. Covered businesses will need to implement tools and procedures to recognize and respond to signals or settings that consumers employ while browsing the internet. Unfortunately, the draft regulations do not provide an exhaustive list of what "user-enabled privacy controls" qualify as valid opt-out requests, adding ambiguity around what is required for compliance. And for covered businesses that use multi-level privacy settings across their site — allowing for different settings in different portions of the site — compliance with this regulation is even more complex. What this means for Internet of Things or other connected services is unclear. (The draft regulations retain a narrow focus on the web/browser environment, while the CCPA applies broadly to many other environments.)

Covered businesses cannot deny an opt-out request based on a lack of verification. The draft regulations confirm that requests to opt out do not need to be verified. Only if covered businesses believe — in good faith — that the unverified request is fraudulent can they deny the request.

Covered businesses must help consumers cure certain deficiencies in their data requests. When consumers submit data access and deletion requests that are verifiable but ignore a covered business's stipulated methods for receiving such requests or are otherwise technically deficient, the business cannot deny the request. The covered business must either fulfill the request or inform the consumer about how the request can be properly submitted.

Covered businesses must treat a deletion request as an opt-out request if a requestor cannot be verified. With respect to deletion requests, if a covered business cannot verify the consumer's identity, it must instead treat the request as one to opt out.

Covered businesses must treat unverified requests for specific pieces of information as requests for categories of information. When a covered business cannot successfully verify a request to access *specific pieces* of information, the business must inform the consumer that their identity could not be verified and then treat the request as if it is seeking the disclosure of *categories* of personal information (rather than deny it outright).

Covered businesses must personalize their responses to requests for access, including requests seeking categorical information. Covered businesses cannot simply link to their privacy policy or rely on a form response when consumers request to know the categories of personal information collected about them, the sources of the information, and with whom it is shared. Instead, covered businesses must provide individualized responses to such requests — with one two-part exception: if the business's response would be the same for all consumers, and the business's privacy policy discloses all the information that needs to be disclosed to the requestor.

Covered businesses must not disclose personal information that will jeopardize the security of the data — and certain data can never be disclosed. A covered business may not produce specific pieces of personal information to consumers in response to access requests if doing so poses a "substantial, articulable, and unreasonable risk to the security of the personal information, the consumer's

account with the business, or the security of business's systems or networks." To avoid security risks, a covered business may *never* disclose Social Security numbers, driver's license numbers or other government-issued identification numbers, financial account numbers, any health insurance or medical identification numbers, account passwords, or security questions and answers to a requesting party.

Covered businesses may execute deletion requests in different ways and must disclose the basis for denying such requests. Upon receipt of a valid deletion request, covered businesses may either de-identify, aggregate, or permanently and completely erase the personal information. When a covered business denies a request for deletion, it must disclose the basis for denial.

Covered businesses must implement a two-step confirmation process for deletion requests. Upon receiving and responding to a verified request for deletion, covered businesses must implement a two-step confirmation process, requiring the consumer to submit the deletion request and then later separately confirm that they want their personal information deleted.

Covered businesses — even those that are exclusively online — must provide a toll-free phone number to receive requests for access. Contrary to the latest CCPA amendments — and thus potentially a dead letter under *Morris* and its progeny as explained above — the draft regulations require covered businesses (with no exceptions) to provide a toll-free phone number to receive requests for access. The draft regulations also state that covered businesses operating a website must implement an "interactive webform" as the second method to receive those same requests. While covered businesses can employ other means outside of a phone number and webform for requests for deletion, most businesses are likely to employ the same methods for both. With time still to make changes, the AG may revise the toll-free phone number requirement in the coming months to comport with the CCPA's language and allow email in lieu of a phone number for certain businesses.

Verification and Consumer Identity

The draft regulations do not dictate the verification procedure — but there's no simple or universal path to a compliant process. In designing a verification process to comply with the law, a covered business must weigh the sensitivity of the data in question, the risk of harm posed by unauthorized disclosure, and the available technology, among other factors. While this flexibility has some positive aspects, in practice, given the severity of the enforcement scheme, the impact for many covered businesses will be incurring the effort (and potentially direct expense) of seeking guidance on a consistent, defensible approach to verifying identity in light of the "specific pieces" of data maintained about a requestor.

Consumers' identities must be verified using existing pieces of information when possible, and covered businesses must delete personal information collected only for verification purposes. Where feasible, covered businesses should avoid collecting new information from consumers in order to verify their identity, and should instead use existing pieces of information. Should a business require additional information from a consumer for identity verification, the business must delete such information "as soon as practical" after processing the request.

Covered businesses can rely on existing password-protected accounts to verify requestors' identities (with re-authentication). For covered businesses receiving requests from consumers who maintain a password-protected account, the businesses may rely on their existing account verification methods when responding to such requests with one addition — consumers must be required to re-authenticate their identity before disclosing or deleting information.

Identity verification poses unique challenges for non-account holders; as a solution, the draft regulations instruct covered businesses to apply a spectrum of confidence. When a consumer does not have an account with a covered business, the draft regulations establish tiers of certainty required for verification. "Reasonable" certainty, where *two* data points must be matched between the consumer and business, is required when a consumer requests disclosure of categories of information. "Reasonably high" certainty, where *three* data points must be matched between the consumer and business, is required when a consumer requests specific pieces of information. Deletion requests may require "reasonable" or "reasonably high" certainty depending on the sensitivity of the data in question and the risk of harm posed by unauthorized deletion.

Covered businesses need to assess which data elements span entire households in order to fulfill household-wide data rights requests. Members of a household (defined by the draft regulations as "a person or group of people occupying a single dwelling") can band together and make joint household data access and deletion requests. Covered businesses must fulfill such requests by providing aggregate household information. Businesses may also respond to joint household requests for deletion by individually verifying the identities of the household members and then complying with the request.

Notices and Privacy Policies

Covered businesses must give notice and obtain explicit consent when planning to reuse personal information they collected for a new, previously undisclosed purpose. A covered business that wishes to use previously collected personal information for a new, previously undisclosed purpose must directly notify the consumer of this new use *and* obtain explicit consent from the consumer to use the personal information for this new purpose. Federal Trade Commission guidance has long recommended this purpose-limitation principle; the draft regulations simply codify it.

Covered businesses must make privacy policies accessible to users with disabilities. Under the draft regulations, privacy policies will be considered valid only if they are accessible to consumers with disabilities or provide instructions about how consumers can access the policy via alternative formats. Privacy policies must also be available in a printable format.

Covered businesses must publish their verification processes in their privacy policy. Covered businesses must describe in their privacy policies the process by which they will verify a consumer rights request and must disclose the specific pieces of information the consumer must provide in their request. For covered businesses that had been planning a quieter, more reactive ("see what comes in the door") approach to verifying data subject requests will need to update their plans. A verification process must be defined and posted in the privacy policy; covered businesses cannot merely invite consumers to send requests to an email address, phone number, or other source.

Covered businesses must disclose how consumers can make requests through an authorized agent. Under the CCPA, authorized agents may make data rights requests on behalf of consumers. The draft regulations require covered businesses to explain in their privacy policy how consumers can designate such an agent.

Covered businesses that do not "sell" person information do not need to disclose the right to opt out. A covered business has no obligation to notify consumers about their right to opt out of the sale of their personal information, *if* the covered business: (i) does not sell personal information during the time the opt-out notice is not posted, and (ii) discloses in its privacy policy that it does not *and will not* sell personal information.

High-volume covered businesses must compile and disclose metrics regarding data rights requests. Covered businesses that alone or in combination annually buy, sell, receive, or share for commercial purposes the personal information of four million or more consumers must compile metrics about how many data rights requests they receive each year, what the outcomes of each kind of request are, and the median number of days needed to process such requests. Such businesses must then disclose those metrics in their privacy policy (or link to them in the policy).

Additional Compliance Requirements

Data rights requests and responses must be recorded and retained. Covered businesses must maintain records of each data rights request received and how the business responded to it going back 24 months. The personal information retained for this purpose cannot be used for any other purpose.

Covered businesses must provide ways to confirm a child's parent/guardian. Covered businesses with actual knowledge that they collect the personal information of children under 13 must establish, document, and provide methods to determine that the person authorizing the sale of the child's personal information is in fact the child's parent or guardian.

The draft regulations further restrict how a service provider can use personal information. The draft regulations state that service providers must not use personal information received from one covered business for the purposes of helping another covered business. Such a limitation may inhibit service providers or vendors from conducting important activities, such as fraud prevention.

Covered businesses that "sell" information collected indirectly from consumers must give or get proof of notice. Covered businesses cannot "sell" personal information supplied by other businesses about consumers — *i.e.*, information not collected directly from consumers — unless the business first (i) confirms that the business supplying the information provided the consumer notice of selling at the time of collection *and* produces signed attestation that it gave such notice, *or* (ii) contacts the consumer directly to provide notice of selling and the consumer's right to opt out. Covered businesses that rely on this type of "selling" face significant and complex compliance burdens.

Covered businesses must explain financial incentives and value of information. For covered businesses that offer a financial incentive to consumers in exchange for them not exercising their CCPA rights, such businesses must notify the consumer about how this incentive works, including an explanation of why it is CCPA-compliant. The businesses must undertake and document "reasonable" and "good faith" methods to determine the value of consumer information, taking into account factors such as the expenses related to or revenue generated from the sale of consumer information.

Covered businesses must train employees on the CCPA and these draft regulations. Covered businesses must train employees who handle consumer requests on all that the CCPA requires with respect to those requests as well as instructions on how to submit such requests.

Final Considerations

The draft regulations may still change and will not be enforceable until July 1, 2020, but enforcement will cover any violations starting on January 1, 2020. Covered businesses that have already put in effort to comply with the CCPA may still need to implement important and significant changes in light of these draft regulations and should not wait until the final regulations are released to take action. Other covered businesses that may be relying on their existing GDPR compliance work are on notice: GDPR compliance does not equal CCPA compliance. Such businesses should conduct a gap analysis right away to identify and remediate where the laws differ.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Michael Rubin
michael.rubin@lw.com
+1.415.395.8154
San Francisco

Robert Blamires
robert.blamires@lw.com
+1.415.395.8142
San Francisco

Scott Jones
scott.jones@lw.com
+1.202.637.3316
Washington, D.C.

Marissa Boynton
marissa.boynton@lw.com
+1.202.637.3307
Washington, D.C.

You Might Also Be Interested In

The California Consumer Privacy Act's Amendments Are Final: What Businesses Need to Know

California Consumer Privacy Act of 2018 May Usher in Sweeping Change

FTC Hearings Discuss the State of Data Security in the 21st Century

FTC Hearing Evaluates Regulatory Oversight of Big Data and Privacy

FTC Opens Doors to New Approaches for Competition and Consumer Protection in the 21st Century

Deep Dive on Deep Learning: FTC Considers Artificial Intelligence

4 Questions to Consider When Dealing With Children's Data in the US

Endnotes

[1] *Morris v. Williams*, 67 Cal. 2d 733, 737 (1967).

[2] *Agric. Labor Relations Bd. v. Superior Court*, 16 Cal. 3d 392, 419 (1976) (citation omitted)); *City of San Joaquin v. State Bd. of Equalization*, 9 Cal. App. 3d 365, 374 (Cal. Ct. App. 1970) ("It is fundamental that an administrative agency may not usurp the legislative function, no matter how altruistic its motives are.").