LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice

February 14, 2020 | Number 2591

What's New, What It Means: California AG Releases Modified CCPA Regulations

While still in draft form, the modifications both clarify certain obligations and introduce new uncertainty for businesses covered by the CCPA.

Key Points:

- On February 7 and 10, 2020, the California AG announced and released modified Proposed Regulations implementing the CCPA.
- The redline version is the quickest means to spot where the California AG has modified the initial draft, which was released last fall.
- Interested parties may submit comments on these new changes no later than 5 p.m. PT on February 25, 2020, by emailing PrivacyRegulations@doj.ca.gov, or mailing the California Office of the Attorney General.[1]
- Key new developments include:
  - What counts as "personal information" has changed. Whether data is personal information now depends on whether the business "maintains the information in a manner that 'identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.'"[2]
  - Restrictions on companies acting as a "service provider" have changed. Service providers can now make internal use of personal information provided by businesses to build or improve the quality of their services, with some restrictions, without disrupting their role as a service provider.[3]
  - The scope of access requests has become broader. The new version of the regulations removed a security exemption for access requests, but businesses can deny requests if a number of factors are met, including that the personal information is not searchable or reasonably accessible and is only maintained for "legal or compliance purposes."[4]
  - Requirements to obtain opt-in consent for new uses of data is now aligned with express FTC requirements. Business must only notify consumers and obtain their explicit consent to any new use that is materially different from those previously disclosed (modifications added "materially different").[5]
  - The obligations around handling unverified deletion requests have changed. Businesses no longer need to treat unverified deletion requests as an opt-out, but now must ask the consumer if they want to opt out of the sale of their personal information.[6]
  - Global privacy controls take precedence over business-specific controls. A "global privacy control," will take precedence over any business-specific controls, but the global privacy

control must "clearly communicate or signal that a consumer intends to the opt-out of the sale of personal information" and cannot be pre-selected.[7]
    - Requirements to "pass down" opt-out have narrowed. Businesses that "sell" personal information must only pass down users' opt-out requests to third parties if they sold personal information between the time the users requested opt-out and the opt-out was implemented (under initial Proposed Regulations, such businesses had to pass down opt-out requests to all third parties to whom they sold personal information in the prior 90 days).

CCPA Basics

The California Consumer Privacy Act of 2018 (CCPA) went into effect on January 1, 2020, and applies to companies doing business with and collecting personal information from California residents (subject to certain thresholds). Among other provisions, the CCPA provides consumers with the following rights over their personal information:

- 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
- The right to know the specific pieces of personal information collected or maintained about them
- The (highly qualified) right to request the deletion of personal information
- The right to opt out of the sale of their personal information
- The right to not be discriminated against for exercising these aforementioned rights

The CCPA 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."[8] The CCPA, however, does not provide a private right of action for any other violation of its other provisions.

The Regulations — Background and Procedure

The California Attorney General (AG) has significant enforcement authority to allege violation(s) of the CCPA against any covered business. The regulations add specificity to this enforcement authority. 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, once final, the regulations will have the same 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.

The California Administrative Procedures Act (APA) governs the process for adopting regulations regarding the CCPA. On October 10, 2019, the AG released the initial draft of the regulations. Under the APA, the initial draft was subject to a public comment period that ended on December 6, 2019. The modified draft regulations were released on February 7 (and again with a brief additional change on February 10) and must be made available for public comment for at least 15 days. The final regulations must be submitted to the Office of Administrative Law (OAL) for final approval, which can take up to 30 "working days." As part of this OAL review process, the AG will have to summarize and respond to each public comment it has received about the draft regulations. After the AG obtains OAL approval, the AG will finalize these regulations by submitting them to the Secretary of State of California.

The CCPA states that the AG "shall not bring an enforcement action under this title for six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is ***sooner***."[9] Even with the onerous timing requirements under the APA, the draft regulations may still go through another round of modifications and comments before July 1, which would mean enforcement of the regulations would begin on or very shortly after the date the final regulations are published.

Modifications to the Proposed Regulations Explained

The modifications have left the initial draft regulations relatively intact. There are, however, significant, substantive changes that will impact who is covered by the law and how covered businesses comply with key aspects of it, including opt-out and access requests.

Key Definitions

Narrowing the Definition of "Personal Information." The modifications provide that whether information is personal information depends on whether the business "*maintains the information in a manner that* 'identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.'"[10] This is a significant change that impacts the analysis of who is subject to the CCPA. Further, the modification changes the question of whether businesses that "maintain" segregated data elements can still "reasonably" link them to a consumer.

Clarifying the Definition of "Household." The definition now requires that to qualify as a household, a person or group must reside at the same residence, share a common device or service, *and* must be "identified by the business as sharing the same group account or unique identifier."[11]

Service Provider

***Expanding How Service Providers Can Use Information*.** The modifications enumerate specific purposes for which a service provider may process personal information,[12] including:

- "[t]o perform the services specified in the written contract with the business."[13] This underscores the critical importance of identifying each service provider, and systematically reviewing and updating written agreements to define the authorized (or prohibited) purposes for processing personal information under CCPA. The key terms and concepts are (in our experience) often not addressed at all, or not well stated, in many agreements. Even data processing agreements drafted to comply with GDPR may need attention for these purposes.
- "internal use by the service provider to build or improve the quality of its services, *provided that the use does not include building or modifying household or consumer profiles*, or cleaning or augmenting data acquired from another source."[14] This addition comes in conjunction with the removal of the initial draft regulations direction that a "service provider shall not use personal information received … for the purpose of providing services to another person or entity." The modification gives service providers clearer direction on permissible uses of information, including at least some greater latitude to use information internally purely for their own benefit.

In addition, the modified regulations state that a service provider may not "sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business," and that "[i]f a service provider receives a request to know or a request to delete from a consumer, the service provider shall either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider."[15]

Many businesses have implemented or are in the process of implementing these opt-outs and request handling processes. Without certainty from a final set of regulations, designing these processes to operate effectively is difficult. And for many businesses, creating these processes is a non-trivial matter, whether that be standing up a manual process or developing an automated method.

Access and Deletion Requests

Access Requests Via Email for Online-Only Businesses. Consistent with the statutory amendments, a business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is only required to provide an email address for submitting access requests.[16] However, this does not displace statutory language mandating that a business (presumably including those that operate exclusively online) must provide two methods for submitting requests to delete.[17]

Exemptions to Right to Access Requirement. The modifications struck the express exception prohibiting a business from providing specific pieces of personal information "if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks."[18]

Now, the modifications provide that a business is not required to search for personal information if ***all*** the following conditions are met:

- The business does not maintain the personal information in a searchable or reasonably accessible format
- The business maintains the personal information solely for legal or compliance purposes
- The business does not sell the personal information and does not use it for any commercial purpose
- The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above[19]

It is not clear what information the AG intended to exempt with this modification, but the net effect of these changes clearly seems to be a narrowing of the articulated exceptions.

Responding to Rights to Delete With Offers to Opt Out. When a business responds to a right to delete request, a business that sells personal information must proactively ask the consumer if they would like to opt out of the sale of their personal information, if (a) they have yet to exercise their opt-out rights, and (b) if such a sale has taken place.[20] The CCPA has so many broadly worded exemptions to the right to delete, this additional requirement (while creating a new burden for businesses) may be an attempt to set this as the default — *i.e.*, the "next best" option for a consumer to end new collections.

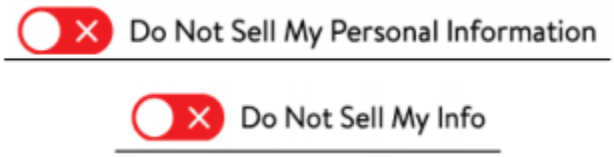
Opt-Out Requests

Changes to How User-Enabled Privacy Controls Must Be Interpreted by Businesses. The new draft regulations specify what qualifies as a privacy control that must be treated as an opt-out: it "shall clearly communicate or signal that a consumer intends to the [*sic*] opt-out of the sale of personal information" and "require that the consumer affirmatively select their choice to opt-out and shall not be designed with any pre-selected settings." Additionally, the new modified regulations introduce the concept of a "global" privacy control. Global privacy controls must be treated as a valid opt-out, and these controls override any "existing business-specific privacy setting."[21]

Narrowing Opt-Out Pass-Downs. Under the original draft regulations, a business that sold information and received a consumer opt-out request was obligated to pass down the request to all third parties to

which it sold information in the prior 90 days. This potentially significant burden has been narrowed in the modified regulations. Now, a business must only pass down opt-out requests if the business sells a consumer's personal information to any third parties *after the consumer submits their request but before the business complies with that request*. Given that businesses must implement the opt-out request within 15 days, this should reduce the number of opt-out pass-downs."[22]

Opt-Out Button. The opt-out button design (provided below) has been finally unveiled. Although there is no requirement to use the button, when used, it should appear to the left of the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link, as shown below, and must be the same size as other buttons on the site.[23] This is a curious design, and goes against a number of accepted best practices in user interface design principles. A toggle switch design is typically used when the user's action will take immediate effect, like a light switch. The label (dictated by the statute itself) is also confusing, and a toggle switch paired with a "do not" statement is particularly unusual.



Notice/Disclosures

Just-in-Time Notice Requirement for Mobile Users. The modified regulations propose a new requirement for just-in-time notices for mobile users before collecting their personal information: "When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection."[24] The modified regulations provide the example of a flashlight application that collects geolocation information (which is both surprising and seemingly unnecessary for delivering the flashlight service). In such a circumstance, the app must provide just-in-time notice of this collection. This aligns the CCPA with current FTC guidance and certain commercial obligations driven by app store terms of service.

Notice at Collection of Personal Information (Via Privacy Policy Link and Otherwise).

- The modified regulations clarify that businesses may provide notice at the point of collection for mobile app users by providing a link to the notice on the app's "download page and within the application, such as through the application's settings menu." This practice is already mandated by major app platforms and state laws. Should a business collect personal information over the phone or in person, notice may be provided orally.[25]
- For call centers and retail locations, scripts and in-store practices may need to be reviewed and adapted, consistent with the business model (*i.e.*, for an online business, the consumer likely has had access to an online policy that states fully all of the information practices, including those pertinent to calls).
- For websites or other online businesses, a conspicuous link to the full privacy statement will still suffice.[26]
- If a separate, shorter document is necessitated by a smaller screen — on, perhaps, smart appliances or smart vehicles — it is not always easy to meet the standards for "readability," particularly while also accounting for the many requirements of a compliant notice (*e.g.*, disclosing all categories of information collected, how it is used, and how it is shared, as well as appropriate data rights).[27]

- Data brokers do not need to provide notice at point of collection if they have provided a link to their privacy policy with instructions on how to opt out in their AG registration submission.[28]

Narrowing of Requirement for Specific Notice of Changes in Use Cases. Under the original draft regulations, businesses had to provide a notice to consumers whenever they were using personal information for a different purpose than the purpose disclosed at collection. Now, a specific notice is required only if the new purpose is "materially different" from the purpose disclosed at the point of collection, consistent with FTC precedent and guidance on these topics.[29]

Disclosing to Whom Data Is Sold. The original draft regulations previously provided that privacy policies must specify the categories of third parties with whom personal information is shared. The modifications have clarified that privacy policies must also specify the categories of third parties to whom each category of personal information is sold.[30]

Elimination of Requirement to List the Sources Specific to Each CCPA Category of Personal Information. Favorably, the modified regulations eliminate the requirement that "[f]or each category of personal information collected, provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information."[31]

Accessibility

Codification of Accessibility Norms for Notices. The original draft regulations added requirements that CCPA notices posted online (privacy policies, notice-at-collection, notice of right to opt out, or notice of financial incentive) had to be accessible to consumers with disabilities. Now, wherever this requirement appears, the modified regulations are clear that the requirement is that the information be "reasonably accessible" and must follow version 2.1 of the World Wide Web Consortium accessibility standards, removing uncertainty about which of the multiple available standards would be deemed sufficient.[32] We (strongly) suggest that every business implement these changes, and we can recommend resources to streamline this process — which hopefully can be accomplished quickly, even as many businesses work to make key features and functionalities of their websites reasonably accessible, in response to the wave of Americans with Disabilities Act class action litigation.

Final Considerations

The modifications to the regulations have materially changed the law, again, and yet there may be another round of modifications before the CCPA's July 1, 2020, enforcement date. The AG has already clearly stated that he will expect compliance with the law as of January 1, 2020, and compliance with the regulations as of the date they become final.

Even as businesses' obligations under the CCPA continue to shift, a new California ballot initiative is under active negotiation with the same stakeholders. This new initiative, which is still subject to significant revisions, likely will be on the ballot in November 2020. This extreme regulatory uncertainty is an inescapable, difficult-to-mitigate reality for companies collecting, sharing, or in any way monetizing, consumer data. For many companies doing business in California, the challenge of rolling out a "CCPA-compliant" privacy program has only become more complicated.

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

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

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

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

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

You Might Also Be Interested In

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

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

Endnotes

1 Lisa B. Kim, Privacy Regulations Coordinator, California Office of the Attorney General, 300 South Spring Street, First Floor, Los Angeles, CA 90013.

2 CCPA Modified Proposed Regulations § 999.302.

3 § 999.314(c).

4 § 999.313(c)(3).

5 § 999.205(a)(5).

6 § 999.313(d).

7 § 999.315(d)(1).

8 Cal. Civil Code 1798.150(a)(1).

9 § 1798.185(c).

10 CCPA Modified Proposed Regulations § 999.302.

11 § 999.301(k).

12 Other enumerated services are: to employ a sub-contractor bound by the same terms the service provider is bound; to detect data security incidents; to protect against fraud or illegal activity; to comply with applicable law; to comply with legal/judicial service; to cooperate with law enforcement investigations; or to exercise or defend legal claims. See § 999.314(c).

13 § 999.314(c)(1).

14 § 999.314(c)(3).

15 § 999.314.

16 § 999.312(a).

17 Id.

18 § 999.313(c)(3).

19 Id.

20 § 999.313(d)(1).

21 § 999.315(d).

22 § 999.315(f).

23 § 999.306(f).

24 § 999.305(a)(4).

25 CCPA Modified Proposed Regulations § 999.305(a)(3).

26 § 999.312(a).

27 § 999.305(b).

28 § 999.301(d).

29 § 999.305(a)(5).

30 § 999.308(c)(1)(e).

31 § 999.308(c).

32 See, *e.g.*, § 999.305(a)(2)(d).