LEGAL UPDATES

The Revised CCPA Regulations: New Provisions Incentivize Early Compliance While Relaxing Key Definitions

On February 7, 2020, the California Attorney General released the second draft of the regulations to the California Consumer Privacy Act (the "CCPA"), followed by an updated version on February 10 (the "Proposed Revisions"), as one revision had been inadvertently omitted from the original release.

02/24/2020 | 7 minute read

On February 7, 2020, the California Attorney General released the second draft of the regulations to the California Consumer Privacy Act (the "CCPA"), followed by an updated version on February 10 (the "Proposed Revisions"), as one revision had been inadvertently omitted from the original release. The Proposed Revisions aim to bring additional clarity to the original draft regulations published on October 10, 2019 (the "Original Regulations"), following a period of substantial commenting. However, even with the new revisions, significant questions on the implementation of the CCPA remain unanswered.

One key takeaway from the Proposed Revisions is that some new language and provisions appear to take aim at businesses currently putting off CCPA compliance until enforcement begins on July 1, 2020. These businesses may therefore want to reconsider this approach. Conversely, some key definitions and restrictions were "relaxing" by the Attorney General in the latest round. A summary of the more significant changes in the Proposed Revisions follows.

Definition of Personal Information

The Proposed Revisions clarify the definition of "personal information" under the CCPA, confirming that whether information constitutes "personal information" depends on whether it is maintained in a manner that identifies, relates to, describes, is reasonably linked, directly or indirectly, with a particular consumer or household. Notably, the example chosen by the Attorney General to illustrate this relates to IP address collection: an IP addresses collected by a business that does not, and could not, otherwise link the IP addresses with a particular consumer or household would not constitute "personal information." This is certainly good news to businesses that only collect information such as IP addresses, which only identifies consumers or households in the aggregate or through inferences from other information. However, businesses that collect multiple data points on consumers will need to evaluate whether such information, in the aggregate or in connection with other information collected by the business, constitutes "personal information." Pending further clarification, in the latter case most certainly, we recommend taking a conservative approach.

Related People

Chiara Portner, CIPP/US

Partner

Redwood Shores

650.804.7672

chiara.portner@lathropgpm.com

Related Services

Data Privacy & Cybersecurity Compliance

Related Sectors

Retail & E-Commerce

The Right to Opt-Out

The right to opt-out is without question a huge source of confusion for both covered businesses and the companies that process personal information for them. It is addressed throughout the Proposed Revisions and yet remains to be fully clarified.

- Perhaps the most significant change in the Proposed Revisions – and one that is sure to incentivize businesses that likely "sell" personal information but have opted to "wait and see" – is the prohibition on selling personal information that was collected in the absence of a posted right to opt-out notice without the consumer's affirmative consent. In other words, if a business claims to **not** sell personal information now, it cannot later sell the personal information previously collected without obtaining consumers' "affirmative authorization."

- Affirmative authorization is currently defined to include a two-step process whereby the consumer must first clearly request to opt-in and then, separately, confirm their choice to opt-in. Given this burdensome requirement, businesses will need to consider whether taking the position that they do not sell personal information may curtail future activities. Note that from the text of the Proposed Revisions it is unclear whether this would prohibit the sale of personal information collected prior to the January 1, 2020 effective date of the CCPA. If adopted as is, the provision would, at a minimum, prohibit the sale of personal information collected after CCPA's January 1, 2020 effective date.

- While we hope that further clarifications on this point will be forthcoming, currently, businesses that sell personal information but have not posted a CCPA-compliant notice of right to opt-out should likely prioritize the adoption of such a notice and consider what personal information was collected without the notice, in order to potentially exclude such information from any personal information sales. Business should also remember that the definition of a "sale" of personal information under the CCPA is broadly defined to include "other valuable consideration", which indicates that many different types of non-cash transactions (or benefits) could classify as potential "sales." Unfortunately, the Proposed Revisions provide little additional clarity on the definition of "sale" of personal information, despite the fact that this definition – one of the cornerstones of the CCPA – is undoubtedly the most unevenly interpreted across the board.

Also introduced with the Proposed Revisions is an optional opt-out button, which businesses may post in addition to posting the notice of the right to opt-out. The button appears as the red toggle switch graphic below. However, given the optional nature of the opt-out button it remains to be seen how many businesses will opt to include it. The graphic provided by the Attorney General has garnered quite the attention given its confusing nature. Suffice to say, it is optional, although if it is used, the business must display the button as mandated under the Proposed Revisions.

Requests to Know and Delete

Another area that generated much discussion following the Original Regulations is the handling of consumer requests. The Proposed Revisions do bring some additional clarity, although in practice this is an area that is likely to remain messy, especially for businesses that are new to handling consumer requests and verification.

- The Proposed Revisions have eliminated the requirement that businesses operating exclusively online and having a "direct relationship" with the consumer provide a web form to submit a right-to-know request. These businesses are now only required to provide an email address. Additionally, the timeframe for responding to requests to know and delete has also been clarified: business are required to acknowledge receipt of a request within ten (10) business days and comply within forty-five (45) days. If the business cannot verify the request within that 45-day period, then the business can deny the request (with an explanation to the consumer, of course). Further, requests denied because a business cannot verify the identity of the requestor no longer need to be treated as valid requests to opt-out of the sale of personal information. Rather, in its response denying the request, the business is required to ask the consumer if he/she would like to opt-out of the sale of his/her personal information.

- Another noteworthy change under the Proposed Revisions is that a covered business is not required to search for information that it (a) does not maintain in a searchable or reasonable accessible format, (b) maintains solely for legal or compliance purposes, and/or (c) does not sell and does not use for any commercial purpose, provided that the business must nonetheless describe to the consumer the categories of records that it did not search.

Mobile Devices and the "Just-In-Time" Notice

Another important change in the Proposed Revisions is the requirement that a business provide a "just-in-time" notice if it collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect. The "just-in-time" notice must contain a summary of the categories of personal information being collected. As such, businesses and application developers that aggressively aim to collect additional data through broad permission requests will now need to disclose what categories of information are being collected, and thus may want to evaluate whether such aggressive collection is worth potentially alienating users who object to such extraneous collection of their personal information. Unlike the GDPR, CCPA does not carry a data minimization requirement, but in practical terms, the need for "just-in-time" notices may serve a similar purpose.

Beyond the "just-in-time" notice, the Proposed Revisions clarify that mobile applications can provide the required notices by providing a link to the notices on the applications download page and within the application itself, including the application's settings menu.

Accessibility

The Original Regulations require covered businesses to provide privacy notices that are accessible to consumers with disabilities, but the Attorney General has until now, provided little guidance as to what is actually required. The Proposed Revisions clarify that such notices should follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1. For those who have not addressed this, web accessibility means ensuring that websites, mobile applications, and other virtual platforms can be used by everyone, including those with disabilities, such as impaired vision. Businesses should evaluate whether their privacy notices meet these accessibility standards. While companies have been working hard to update their notices to comply with CCPA, this requirement has, by and far, slipped through the cracks, though it is certain to generate some discussion (if not litigation) in coming months, as there has been an explosion in recent years of web accessibility lawsuits based on the American Disabilities Act.

Data Broker Notice Requirements

The Proposed Revisions have eased the notice requirements for data brokers, clarifying that businesses that do not collect information directly from consumers, but register with the Attorney General as a data broker, do not need to provide a notice to a consumer at collection **if** the data broker has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out.

Service Providers

Service providers are a key element of CCPA, but determining how service providers may use personal information has been a bit of challenge under CCPA. The Proposed Revisions appear to answer some of the questions and relax some of the earlier restrictions.

- During the commenting period, many comments and requests for clarification zeroed in on how service providers could use personal information, particularly with respect to section 999.314 of the Original Regulations. In fact, one request that popped up repeatedly was for service providers to be able to use the personal information processed on behalf of covered businesses for internal analytics, debugging and product improvement. This appeared to be prohibited under the Original Regulations, despite the fact that anyone in the software industry understands the need for this. The Attorney General now appears to have conceded to this important point. As such, in the Proposed

Revisions, the restrictions on service providers' use of personal information and their obligation to delete such information have been lessened. Service Providers may additionally use personal information:

- For internal use by the service provider to build or improve the quality of its services, if such use does not include the building or modifying of household or consumer profiles, or cleaning or augmenting data acquired from another source; and
- to detect data security incidents or protect against fraudulent or illegal activity.
- Further, the Proposed Revisions also clarify that a business providing services to an entity that is not regulated by the CCPA but that would otherwise meet the requirements and obligations of a service provider will be considered a service provider under the CCPA. As such, businesses acting as vendors for non-regulated entities should likely consider updating their contracts to include language required by CCPA for service providers – and ensuring that those agreements allow for the "other" uses set forth above.
- Many adtech companies (ad networks and intermediaries) have taken the unlikely position that they are service providers, and that no sale is involved. However, it appears that this position is no longer tenable under the Proposed Revisions, which specifically state that the use (of personal information by a service provider) must **not** include *the building or modifying of household or consumer profiles, or cleaning or augmenting data acquired from another source*. There is no question that many in the adtech industry would have preferred that the Attorney General take a more forthright position on targeted advertising, but this may be as clear as it will ever be, at least until enforcement begins.

Next Steps

The Attorney General's office is currently accepting written comments on the Proposed Revisions, which may be submitted to the Attorney General until 5:00 pm on February 25, 2020. The draft regulations will likely be finalized this spring. Until then, businesses should continue to watch for any additional changes to the draft regulations or any additional guidance from the Attorney General. In the meantime, covered businesses that have put CCPA compliance on hold – particularly those that sell personal information – ought to get busy updating their notices and ensuring that opt-out notices are provided to consumers, so as not to be left with "unusable" data.

If you have any questions about CCPA, or any other issue relating to data privacy, please contact:

Chiara Portner