GIBSON DUNN

# California Consumer Privacy Act Update: Attorney General Proposes Regulations Version 2.0

Client Alert | February 19, 2020

---

On February 7, 2020, California Attorney General Xavier Becerra released a revised set of proposed regulations for the California Consumer Privacy Act of 2018 ("CCPA"), and released an additional amendment on February 10, 2020.[1] These proposed regulations provide further details and clarifications on the steps businesses must take to comply with the CCPA. This is not the end of the road for the development of the regulations, however, as the Attorney General will at least consider additional comments, which must be submitted by February 25, 2020, before the regulations are finalized.[2]

The CCPA[3] took effect January 1, 2020, and aims to give California consumers increased visibility into and control over how companies use and share their personal information. It applies to all entities doing business in California and collecting California consumers' personal information if they meet certain thresholds. The Attorney General's power to enforce the law is delayed until July 1, 2020. More information can be found in our prior client alerts on the topic, including a summary of the statute (here), amendments from October 2018 (here), additional proposed amendments (here), the Attorney General's draft regulations (here), the final amendments signed in October 2019 (here), and a summary of CCPA developments heading into 2020 (here).

The revised version of the proposed regulations adjusts some of the requirements imposed on businesses by the initial proposed regulations, clarifies certain definitional ambiguities, and includes additional proposed provisions relating to service providers' handling of personal information.

Below, we briefly summarize a number of the key changes in the revised proposed regulations. The list is not exhaustive, and we encourage you to contact us with any questions. As the public comment period is an important opportunity for companies to provide feedback to shape the proposed regulations, please feel free to contact any of the Gibson Dunn attorneys listed below if you are interested in submitting comments in advance of the February 25, 2020 deadline.

## Key Definitions Clarified

- ***"Personal information"***: Version 2.0 of the proposed regulations ("Version 2.0") adds guidance for interpreting the definition of "personal information" under the CCPA, alleviating some concern regarding exactly how broadly "personal information" would be applied. Specifically, whether information constitutes "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 reasonably be linked, directly or indirectly, with a particular consumer or household."[4] The revised regulations clarify that IP addresses—which have been a particular focus for companies collecting statistical and analytical information on the usage of their websites—that

### Related People

Ryan T. Bergsieker

Cassandra L. Gaedt-Sheckter

Abbey A. Barrera

are not tied to any identifiable consumers or households, and that cannot be reasonably linked to any identifiable consumer or household, do not constitute "personal information" under the CCPA in those instances.[5]

- ***"Categories"***: Version 2.0 clarifies that businesses must describe "categories of sources"[6] and "categories of third parties"[7] to consumers in notices at collection, privacy policies, and in response to verified requests to know with "enough particularity to provide consumers with a meaningful understanding of the type" of source or third party.

## Notices At Collection Must Be Readily Accessible

The revised regulations update obligations related to notices at collection, particularly with respect to mobile applications. For instance, the regulations state notices must be posted wherever personal information is collected, including on webpages, mobile application download pages (and within mobile applications, such as the settings menu), and printed forms.[8] Furthermore, businesses must provide consumers with a "just-in-time" notice, describing the categories of personal information being collected and a link to the full notice at collection, when collecting personal information that consumers would "not reasonably expect" to be collected from mobile devices.[9] If personal information is collected orally, oral notice may be given.[10] In addition, the draft provides the following regarding notices:

- ***No Additional Consent Required For Use Not "Materially" Different***

Version 2.0 makes clear that additional consent is not required for the use of previously collected personal information that is not "materially" different from the uses disclosed in the original notice at collection. Under the previous iteration of the proposed regulations, any additional use of personal information that did not fall strictly into the uses described in the notice at collection would have required the business to seek additional consent.[11]

- ***Specific Business Or Commercial Purpose Need Not Be Explicitly Tied To The Category Of Personal Information***

The revised regulations no longer require a business to identify the specific business or commercial purpose for the collection of *each* category of personal information collected.[12] In other words, Version 2.0 suggests it is sufficient simply to list the business or commercial purposes for collecting all the categories of personal information collected, and a breakdown by category is no longer necessary. This revision is similarly explained in the section of Version 2.0 on Privacy Policies.[13]

- ***Data Broker Obligations Simplified***

Data brokers registered with the Attorney General under California's data broker registration law (Civil Code § 1798.99.80) that post links to their privacy policies containing instructions on how to opt-out need not provide notices at collection.[14] This provision replaces the previously proposed mandates requiring businesses not collecting personal information directly from consumers to either (1) contact consumers directly to provide notice, or (2) contact the source of the information for an attestation describing how the source provided the required notice at collection (this provision was discussed in more depth in our previous client alert regarding the first draft of the regulations, available here). However, the new provision leaves unclear how "data scrapers" that do not *sell* personal information—or simply companies that obtain non-exempted personal information from sources other than the consumer, such as publicly available sources other than government records—should provide notice to the consumer.

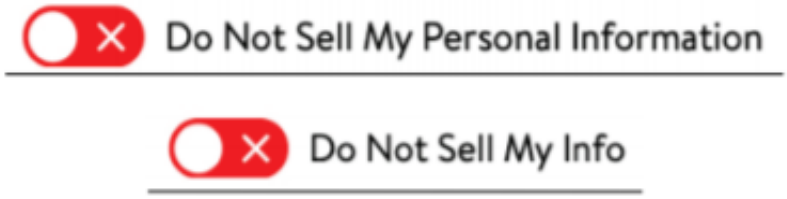
- ***Employee Notice Explained***

The notice at collection provided to employees does not need to include a "Do Not Sell My

Personal Information" link, and may include a link to (or a paper copy of) the employee privacy policy, instead of the general consumer privacy policy.[15]

## "Do Not Sell" Provisions And Optional Opt-Out Button

Version 2.0 provides an option to obtain user consent to sell data that the business collected during the time it did not have a notice of the right to opt-out, as opposed to the total ban of that sale under the previous version of the proposed regulations.[16] The new draft regulations also give the *option* of providing an "opt-out" button alongside the "Do Not Sell My Personal Information" link, and provide a visual depiction of how such a button may appear (see below), but requires the link nonetheless.[17]




## Responding To Requests To Know And Requests To Delete

- ***Required Response Time Revised***

Under the new proposed regulations, businesses are required to confirm receipt of requests to know and requests to delete within 10 ***business*** days—instead of "10 days"—though the allowed period to respond to the requests remains 45 ***calendar*** days.[18]

- ***Designated Methods For Submitting Requests Simplified***

The updated proposed regulations eliminate the requirement to maintain a webform. Businesses that operate solely through a website must provide an email address to submit requests to know, but no longer need to additionally maintain a webform. All other businesses must provide at least two designated methods for submitting requests to know, including at a minimum a toll-free number.[19] The requirement to provide two designated methods for submitting requests to delete (which do not necessarily include a webform), remains unchanged.[20]However, the proposed regulations indicate that businesses should still consider the ways in which they primarily interact with consumers when providing additional methods for submitting requests.

- ***Exemption For Businesses That Do Not Sell And Only Maintain Personal Information For Legal Compliance***

In response to consumers who make requests to know the personal information a business has collected about them, Version 2.0 relieves businesses of the requirement to search for personal information if the following conditions are met: 1) the business does not maintain personal information in a searchable or reasonably accessible format; 2) the business maintains the personal information solely for legal or compliance purposes; 3) the business does not sell personal information and does not use it for any commercial purpose; and 4) the business describes to the consumer the categories of records that may contain personal information, despite not having searched because it meets the above conditions.[21]

- ***Biometric Information Should Not Be Provided In Response To Requests To Know***

In response to requests to know, biometric information joins other categories of sensitive information that businesses cannot disclose, such as Social Security numbers and financial account numbers. Biometric data includes such information either generated from measurements or technical analysis of human characteristics. This is consistent with the legislature's recent revision of the categories of information that trigger breach notice requirements, and consequently, the relevant categories of personal information subject to the private right of action under the CCPA.

- ***Unverified Requests To Delete Do Not Need To Be Treated As Opt-Out Of Sales***

Unlike the previous draft of the proposed regulations, businesses no longer need to treat unverified requests to delete as opt-out of sales of personal information. Instead, businesses are permitted to *ask* consumers if they would instead like to opt-out of the sale of their personal information, provided they had not already made a request to opt-out.[22]

- ***Businesses Can Retain Record Of Requests To Delete***

Version 2.0 explicitly allows businesses to retain a record of the request for the purpose of ensuring the consumer's personal information remains deleted from the business's records.[23]

- ***Verification For Requests from Households With Minors***If a member of the household is a minor under the age of 13, the business must obtain verifiable parental consent before complying with requests to access or delete specific pieces of information for the household.[24]
- ***Verification For Non-Account Holders***

Version 2.0 provides additional examples of acceptable methods for verifying consumers who do not have password-protected accounts, including asking the consumer to respond to in-app questions, or provide additional information about a transaction amount or an item purchased.[25]

- ***Authorized Agent Requests***

The new draft regulations allow businesses to require agents to submit a *signed* permission and consumers to directly confirm the authorization of the agent with the business, and impose additional requirements on authorized agents, such as implementing and maintaining reasonable security to protect consumers and restricting their use of the information.[26]

## Service Providers Are Granted Greater Leeway

Version 2.0 no longer bars service providers from using the personal information they collect for their own purposes, so long as the personal information is not used to build household or consumer profiles or "clean or augment the data with data acquired from another source."[27]

Furthermore, in response to requests to know or delete, service providers can either act on behalf of the business or inform the consumer that the request cannot be processed because they are a service provider.[28]

## Clarifications Regarding Requests To Opt-Out

The updated regulations now allow businesses to propose an opt-in, after consumers have already opted-out of the sale of their personal information, if those consumers have attempted to use a product or service that requires the sale of their personal

information.[29]

## Recordkeeping Requirements Lessened

Version 2.0 changes the threshold triggering the recordkeeping requirement for businesses that collect, use, or disclose the personal information of large numbers of consumers within one year.[30] The threshold for triggering the recordkeeping requirement was increased from the collection of information from 4 million consumers to 10 million consumers. Businesses that meet the 10 million threshold must compile and disclose within their privacy policy the numbers for all requests to know, delete, and opt-out received for all individuals. Though the initial draft regulations required those businesses to report the number of requests received from California residents (consumers) specifically, Version 2.0 grants the option of disclosing the number of requests received from all individuals, eliminating the added effort that may be required to parse out California residents.[31]

## Conclusion

Version 2.0 of the proposed CCPA regulations provides some much needed clarification on certain of the ambiguities in the CCPA. However, not all ambiguities have been resolved. For example, the new draft regulations do not provide any practical clarity on the prohibition of the use of personal information for the purpose of building a “consumer” or “household profile” by service providers.

Companies subject to the CCPA should continue to monitor the proposed regulations as they evolve. It is also important to provide comments and weigh in by February 25, 2020 on issues of interest to particular companies that remain unclear. We are available to assist with your inquiries as needed.

---

[1] The entire text of the draft regulations is available at https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-redline-020720.pdf?.

[2] Department of Justice, Title 11, Division 1, Chapter 20. California Consumer Privacy Act Regulations (February 10, 2020), available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-notice-of-mod-020720.pdf.

[3] The CCPA is encoded in California Civil Code Sections 1798.100 to 1798.198.

[4] Draft Regulations § 999.302(a) (emphasis added).

[5] Id.

[6] Draft Regulations § 999.301(d).

[7] Draft Regulations § 999.301(e).

[8] Draft Regulations § 999.305(a)(3).

[9] Draft Regulations § 999.305(a)(4).

[10] Draft Regulations § 999.305(a)(3)(d).

[11] Draft Regulations § 999.305(a)(5).

[12] Draft Regulations § 999.305(b)(2).

[13] Draft Regulations § 999.308(c)(1)(d).

[14] Draft Regulations § 999.305(d).

[15] Draft Regulations § 999.305(e).

[16] Draft Regulations § 999.306(e).

[17] Draft Regulations § 999.306(f).

[18] Draft Regulations § 999.313(a).

[19] Draft Regulations § 999.312(a).

[20] Draft Regulations § 999.312(b).

[21] Draft Regulations § 999.313(c)(3).

[22] Draft Regulations § 999.313(d)(1).

[23] Draft Regulations § 999.313(d)(3).

[24] Draft Regulations § 999.318(c).

[25] Draft Regulations § 999.325(e).

[26] Draft Regulations § 999.326(a), (e).

[27] Draft Regulations § 999.314(c). Please note that “household or consumer profiles” are not defined.

[28] Draft Regulations § 999.314(e).

[29] Draft Regulations § 999.316(b).

[30] Draft Regulations § 999.317(g).

[31] Id.

---

The following Gibson Dunn lawyers assisted in the preparation of this client update: Alexander Southwell, Ryan Bergsieker, Cassandra Gaedt-Sheckter, Abbey Barrera, and Lisa Zivkovic.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, or any member of the firm's California Consumer Privacy Act Task Force or its Privacy, Cybersecurity and Consumer Protection practice group:

**California Consumer Privacy Act Task Force:**
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Cassandra L. Gaedt-Sheckter - Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Alexander H. Southwell - New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Deborah L. Stein (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)

Please also feel free to contact any member of the Privacy, Cybersecurity and Consumer Protection practice group:

**United States**
Alexander H. Southwell - Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin - New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Deborah L. Stein (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

**Europe**
Ahmed Baladi - Co-Chair, PCCP Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox - London (+44 (0)20 7071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Bernard Grinspan - Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)

**Asia**
Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)



## Related Capabilities

Privacy, Cybersecurity, and Data Innovation