ALSTON & BIRD

WWW.ALSTON.COM

Privacy & Data Security ADVISORY ■

OCTOBER 14, 2019

The Draft CCPA Regulations: 21 Potentially Significant Business Impacts

By Jim Harvey, David Keating, and Dan Felz

On October 10, 2019, California Attorney General Xavier Becerra released Proposed Regulations (the "Regulations") for the California Consumer Privacy Act ("CCPA"). These Regulations are intended to operationalize the CCPA and provide clarity to assist in the implementation of the law. The Regulations contain guidance on a number of CCPA topics of vital importance to companies, including notices, consumer requests, do not sell rules, and data-mediated financial incentive programs.

The CCPA enters into effect on January 1, 2020. The Regulations that the Attorney General has proposed will not become effective at that time. Instead, the Attorney General will hold four public hearings to address these regulations on December 2, 3, 4, and 5, 2019. The written comment period will then end on December 6, 2019. The CCPA requires the Attorney General to adopt initial regulations on or before July 1, 2020. Thus, the Regulations would presumably enter into force on or around July 1, 2020.

Still, companies should be aware that the Regulations could potentially be read as interpretations of the CCPA when it comes into effect on January 1, 2020. Thus, some of the issues discussed below could potentially have indirect effects before the July 2020 timeframe when they are slated to enter into force.

In this Advisory, we summarize the portions of the Regulations that are likely of material interest to companies across industries. Issues are arranged by topic: (a) privacy notices and the online privacy policy, (b) opt-outs / do not sell requests, (c) rights requests generally, (d) access requests, (e) deletion requests, (f) service providers - data use restrictions.

Privacy Notices and the Online Privacy Policy

1. The need for just-in-time notices beyond the online Privacy Policy.

The Regulations distinguish between two types of notice in the CCPA:

- First, Section 1798.100(b) of the CCPA requires a "notice" to be provided "at or before the point of collection." (For convenience, we refer to this as the "100(b) Notice".)
- Second, Section 1798.130(a)(5) of the CCPA requires a comprehensive privacy policy to be posted on a business's website. (Here, we describe this as the "online Privacy Policy.")

The Regulations present a position that may come as a surprise to some companies: Simply having an online Privacy Policy posted on their websites is *not* sufficient to satisfy companies' CCPA notice responsibilities.

Instead, in addition to having an online Privacy Policy, companies must provide additional, just-in-time 100(b) Notices at every specific data collection point – or forgo collecting data there entirely. Additionally, data uses are limited to what is disclosed at the point of collection. In brief detail:

- The "notify at each collection point, or do not collect data there" rule. The Regulations state that if a business "does not give [] notice at collection to the consumer at or before the collection of their personal information," it "shall not collect personal information from the consumer."[1]
- The "uses are limited to what you notify at collection" rule. Under the Regulations, "a business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection." Instead, any new uses require "explicit consent."[2] (This provision of the Regulations resembles the "purpose limitation" principle of European data protection law, codified in Article 5(1)(b) GDPR.)

What needs to be in these point-of-collection notices? At the least:

- The categories of data to be collected.
- The business or commercial purposes for which data will be used.
- If the business sells personal information, a "do not sell my info" link.
- A link to the business's online Privacy Policy.

Furthermore, these just-in-time 100(b) Notices must be "visible and accessible where consumers will see it before any personal information is collected"[3] – taking account of "smaller screens" where applicable.[4] They must also be "accessible to consumers with disabilities."[5]

If the Regulations were to require just-in-time notices at every single point of data collection, this would raise a number of questions across industries. Retailers with brick-and-mortar stores will need to examine in-store data collection, including loyalty sign-ups, CCTV signage, and in-store traffic analytics. Point-of-sale devices also collect payment card data, potentially engaging the Regulation's notice provisions. Call centers and customer-service interactions represent another area of potential focus.

It is also unclear whether websites could simply operate as they always have, with a link to their online Privacy Policy on the bottom of their pages – or whether a new "we collect your data"-style notice banner would be required "before any personal information is collected." This also contributes to the discussion of whether cookie banners are now required, or at least advisable, to comply with CCPA notice requirements.

Operationally, this provision of the Regulations requires businesses to raise flags with their IT departments or IT vendors, start identifying data collection points, and start discussing what kind of notice builds may be necessary.

2. Nondiscrimination rights need to be in the online Privacy Policy.

As companies began drafting CCPA amendments to their privacy notices, some raised the question of whether the CCPA's non-discrimination provisions constituted consumer "rights" that had to be explained

---

1 Regulations § 999.305(a)(5).

2 Regulations § 999.305(a)(3).

3 Regulations § 999.305(a)(2)(e).

4 Regulations § 999.305(a)(2)(b).

5 Regulations § 999.305(a)(2)(d).

in their online Privacy Policy. The Regulations now make it explicit that the Privacy Policy must "explain that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights."[6]

3. Financial incentive programs need "financial incentive notices." These notices need to include (a) "this is the value of your data" estimates, and (b) the methodology that was used to arrive at them.

When companies offer financial incentives, the Regulations require them to provide a specific "notice of financial incentive." These notices must contain the following specific information about the incentive program:

- *A "good-faith estimate" of the "value of the consumer's data that forms the basis for offering the financial incentive."*
- *"A description of the method the business used to calculate the value of the consumer's data."*[7]

The Regulations also contain an exhaustive list of methods that businesses "shall" use to calculate the value of consumers' data.[8] These include the "marginal value to the business" of consumer data;[9] "[r]evenue or profit generated by the business from sale" of consumer data;[10] and "[e]xpenses related to the sale" of consumer data.[11] We anticipate that this provision will receive extensive comments, since this modeling may be more complicated than it first appears, and difficult to defend if challenged.

This rule is likely of interest to any companies that operate loyalty programs. Also, online publishers who offer both paid subscriptions and 'free' (i.e., paid by advertising) modules may potentially need to consider these rules. Data-mediated financial and insurance products could also require review, such as pay-as-you-drive insurance, safe-driving discounts, and the like.

4. Larger companies have to track CCPA request metrics and disclose them in their online Privacy Policy.

Under the Regulations, any business that annually "buys, receives, sells, or shares" personal information of 4 million or more consumers would have to:

- *Track the number of access, deletion, and opt-out requests it receives annually and its median response times to those requests.*
- *Disclose these statistics in its online Privacy Policy.*[12]

It is unclear whether a business would only trigger this rule by processing personal information relating to 4 million *California* consumers, or if processing data of 4 million consumers from anywhere in the U.S. would be sufficient. If the latter, many companies could potentially have to start maintaining CCPA metrics. Companies of almost any size could be covered by this provision of the Regulations.

---

6 Regulations § 999.308(b)(4)

7 Regulations § 999.307(b)(5).

8 *See* Regulations § 999.337(b).

9 Regulations § 999.337(b)(1).

10 Regulations § 999.337(b)(3).

11 Regulations § 999.337(b)(5).

12 Regulations § 999.317(g).

Of course, these statistics may be manageable for businesses that maintain a ticketing system for CCPA requests, so long as those systems are tracking CCPA requests by request type and recording time to closure.

5. When businesses do not collect personal information directly from consumers, they cannot sell it without either (a) documenting diligence in their data sourcing or (b) providing consumers with a notice of sale and an opt-out.

One of the trickier notice rules under the GDPR was Article 14, which requires that companies collecting personal information from sources other than the affected consumer have to provide privacy notices to those consumers. As the Regulations were being drafted, there was some discussion of whether they would adopt Article 14 GDPR's approach to notice.

The Regulations did not do so. Instead, they expressly state that "[a] business that does not collect information directly from consumers does not need to provide a notice at collection."[13]

At the same time, however, the Regulations restrict the onward sale of any personal information that businesses do not collect directly from consumers. Such personal information cannot be sold unless the business either:

- Contacts its third-party data sources and "[o]btain[s] signed attestations from the [data] source describing how the source gave the notice at collection and including an example of the notice" – and make this notice available to the consumer upon request.
- "Contact[s] the consumer directly to provide notice that the business sells personal information about the consumer," while also notifying the consumer about his right to opt-out.[14]

This rule is likely to be of particular interest to data providers, who may need to adjust their data diligencing procedures to accommodate this rule. However, many other companies purchase data for marketing purposes in the normal course of their business, such as purchasing third-party audiences to power targeted display advertising or social media marketing campaigns.

It is unclear whether these activities would trigger heightened data-sourcing or consumer-notice requirements under the current draft of the Regulation. This could potentially be a concern, for example, to the extent providing audience segments to third-party advertising technology vendors is considered a "sale" of data under the CCPA. It is also unclear what needs to happen at a "second-level sale," i.e., when a company buys data from a data broker who bought it from someone else. Would the company need to check only the data broker's privacy notice and obtain only the broker's signed attestation as to how data was collected, or go "through" the data broker and check the notices of parties that may have originally collected the data it is leasing, as well as the signed attestations the broker obtained describing how data was originally collected?

Rights Requests Generally

6. When rights requests are made, confirmation of receipt is mandatory.

Under the Regulations, when a business receives an access or deletion request, it would have to "confirm receipt of the request within 10 days and provide information about how the business will process the

---

13 Regulations § 999.305(d).

14 Regulations § 999.305(d).

request" – including how the identity verification process works.[15] Many businesses were already building these kinds of automated confirmations as part of their CCPA implementation programs. The Regulations would make them mandatory.

7. Companies with significant brick-and-mortar consumer interactions (e.g., retailers) need to accept offline CCPA requests.

The Regulations contain a special rule for businesses that "operat[e] a website but primarily interac[t] with customers in person at a retail location." Such businesses would have to offer in-store consumers "a form that can be submitted in person at the retail location" to make CCPA rights requests.[16] Similarly, businesses that "substantially interac[t] with consumers offline" must "also provide notice to the consumer by an offline method" that "facilitates consumer awareness of their right to opt-out."[17] These rules require that companies with brick-and-mortar locations accept CCPA requests offline – and have appropriate forms ready at retail locations to facilitate them.

8. Businesses have to retain records of the CCPA rights requests they receive from consumers for 24 months.

The Regulations establish a 24-month retention requirement for records relating to CCPA rights requests.[18] Of course, subject to appropriate security, businesses could retain them for a longer period if they think such records may be relevant for litigation or compliance.

9. Businesses need a documented ID verification method, and it must follow a risk-adjusted security scale based on the data involved. Third-party tools and account logins are permitted, as long as they provide adequately secure ID verification.

One key CCPA topic is how companies verify the identity of individuals who submit CCPA requests. The Regulations require companies to "establish, document, and comply with" a "reasonable method for verifying that" the person making a CCPA request is "the consumer about whom the business has collected information."[19] This ID verification method should be built as follows:

- ID verification procedures must include a risk-adjusted scale. ID verification should be tailored to the "type, sensitivity, and value of the personal information collected" about the consumer.[20] If data is sensitive, is valuable, poses harm to the consumer if deleted, or is likely to be targeted by malicious actors, ID verification procedures must be more stringent.
- Password-protected account logins are ok if they offer sufficient security: The Regulations permit companies to use logins to password-protected accounts to verify consumer identities, provided that the login provides the appropriate level of verification on the risk-adjusted scale outlined above.[21]

---

15 Regulations § 999.313(a).

16 Regulations § 999.312(c)(2).

17 Regulations § 999.306(b)(2).

18 Regulations § 999.317(b).

19 Regulations § 999.323(a).

20 Regulations § 999.323(b)(3)(a).

21 Regulations § 999.324(a).

- Third-party tools permitted: The Regulations also permit businesses to use third-party tools for ID verification.[22] Of course, these tools must provide appropriate authentication under the Regulations' general risk-adjusted scale for ID verification.
- Fraud prevention required: The Regulations require businesses to implement "reasonable security measures to detect fraudulent identity-verification activity."[23]

10. All personnel who handle CCPA requests need CCPA training, as well as employees responsible for CCPA compliance.

The Regulations require businesses to "[e]stablish, document, and comply with a training policy" for CCPA training. Personnel must receive CCPA training if they (a) are responsible for handling CCPA consumer requests, or (b) are responsible for the business's compliance with the CCPA.[24]

Many companies have already started developing CCPA training materials and training plans. This portion of the Regulations would require an express CCPA training policy, and documentation that the right portions of the organization have received their CCPA training.

Opt-Outs / "Do Not Sell My Data" Requests

11. Opt-out requests do not need to be "verifiable consumer requests."

The CCPA requires access and deletion requests to be "verifiable consumer requests," where businesses verify the ID of consumers prior to execution. For opt-out requests, however, the Regulations provide they "need not be a verifiable consumer request."[25] It is unclear whether this means that opt-out requests must be executed even without proof of identity – the Regulations merely state that opt-out requests can be denied if companies have a "documented belief" that the opt-out request is "fraudulent."[26] It seems apparent, however, that the Regulations envision a lower ID verification threshold for valid opt-out requests than for valid access or deletion requests.

12. Businesses have 15 days to execute a "Do Not Sell My Info" request.

The text of the CCPA itself does not contain a time limit in which opt-out/do-not-sell requests must be executed. This gave rise to questions about whether they had to be executed immediately upon receipt. The Regulation clarifies that opt-outs must be executed within 15 days of receipt.[27]

13. Do-Not-Sell requests need to be flowed down to all "purchasers" of the data from within the last 90 days.

The CCPA did not address whether businesses that receive opt-out requests must provide them to third parties that have received data relating to the consumer making the opt-out. This stood in contrast to Deletion requests, for example, which the CCPA expressly required to be flowed-down to service providers.

---

22 Regulations § 999.323(b)(1).

23 Regulations § 999.323(d).

24 Regulations § 999.317(g)(3).

25 Regulations § 999.315(h).

26 Regulations § 999.315(h).

27 Regulations § 999.315(e).

The Regulations attempt to address this issue. They require businesses that receive opt-outs to "notify all third parties" to whom they have sold the consumer's personal information "within 90 days prior to the business's receipt of the consumer's" opt-out request. The business must further instruct these third parties "not to further sell the information." Once this is done, the business must "notify the consumer" that third-party notification is complete.[28]

It is unclear how this rule is envisioned to work in practice. Opt-outs do not need to be "verifiable" consumer requests, so a business may not know the full identity of consumers who request opt-outs. Further, by CCPA definition, third parties that receive "sales" of consumer data are not "service providers" subject to the instructions of the business. It is therefore unclear whether "instructions" that the business issues to these third parties must be followed – and what the consequences are for the business if they are not.

14. Do Not Track is back … as a Do-Not-Sell request?

The Regulations require businesses that collect personal information online to "treat user-enabled privacy controls" – such as "a browser plugin or privacy setting or other mechanism that communicate or signal the consumer's choice to opt-out of the sale of their personal information" – as "a valid [opt-out] request."[29]

This could potentially be read as stating that a browser's Do Not Track setting should be treated in the same manner as a Do-Not-Sell / Opt-Out request, and executed accordingly by any company that has a website. If so, this rule could cause significant disruption. The law in force to date has not required any websites to respond to Do Not Track signals – nor are such signals uniform. Of course, this provision of the Regulations could also be read as encouraging the development of market-standard mechanisms for "signal[ing] the consumer's choice to opt-out of the sale" of data.

Access Requests

15. Despite access requests, specific pieces of information can be withheld on security grounds.

Even if a consumer makes an access request, the Regulations would permit businesses to withhold pieces of personal information if they create a "substantial, articulable, and unreasonable" risk to the security of: (a) the personal information itself, (b) the consumer's account with the business, or (c) the business's systems or networks.[30] This is a potentially welcome clarification for businesses. Section 1798.150 of the CCPA arguably imposes a duty for businesses to implement "reasonable security," and it would have been difficult to comply with this duty if access requests could be used to require businesses to disclose information that poses security risks.

16. Businesses can never disclose Social Security number, driver's license number, government-issued ID number, financial account number, health insurance or medical ID numbers, account passwords, or security questions and answers.[31]

The Regulations contain a list of data fields that businesses cannot disclose to consumers "at any time," even if the consumer has made an access request.

---

28 Regulations § 999.315(f).

29 Regulations § 999.315(c).

30 Regulations § 999.313(c)(3).

31 Regulations § 999.313(c)(4).

Deletion Requests

17. Deletion requests submitted online need a "double opt-in."

The Regulations require companies that receive Deletion request to go back to the consumer, and obtain a *second* confirmation that the consumer wants her information deleted. In the Regulation's words, a business "shall use *a two-step process* for online requests to delete":

- First, the consumer must "clearly submit the request to delete."
- Second, the consumer must "separately confirm that they want their personal information deleted."[32]

This double-confirmation requirement cuts across industries, and would be another item for IT's list of CCPA project builds. Although it is not required for deletion requests made "offline," companies may be well advised to obtain a separate confirmation for offline deletion requests as well.

18. "Sorry, we can't verify your ID" denials of deletion requests must be automatically converted into Do-Not-Sell requests.

If a business receives a consumer deletion request, it is permitted to deny the request if it cannot adequately verify the requestor's identity. In such a case, the Regulations would nonetheless require the business to "instead treat the request as a request to opt-out of sale."[33]

Implementing this provision could be difficult. For one, opt-out requests – unlike access and deletion requests – do not need to be ID-confirmed "verifiable consumer requests" (as discussed above). Thus, at least theoretically, a deletion request where ID verification fails could potentially be converted into an opt-out. Still, it is unclear how businesses would be able to take information about a person whose identity they cannot verify, and use it to stop "selling" that person's data as defined under the CCPA. This could be particularly true in cases where, as GDPR practice has shown, requestors abandon their requests at an early stage.

19. Archived data is out-of-scope for deletion requests (unless the archives get restored into production).

The Regulation states that for personal information stored on "archived or backup systems," businesses would be able to "delay compliance with the consumer's request to delete … until the archived or backup system is next accessed or used."[34] This would likely be a welcome clarification to many businesses, since backups or archives may not permit deletion of data as a technical matter.

20. When a business relies on a statutory exception to consumers' deletion rights, it cannot use that data "for any other purpose than provided for by that exception."

The CCPA permits consumers to request deletion of their data, but balances this with a number of exemptions businesses can rely on to retain data despite the consumer having made a deletion request.[35] The Regulations now propose that when businesses rely on CCPA exemptions to consumer deletion rights, they would only be permitted to use that data for the purpose specified in the relevant CCPA exemption.[36] For example, if

---

32 Regulations § 999.312(d).

33 Regulations § 999.313(d)(1).

34 Regulations § 999.313(d)(3).

35 *See § 1798.105 CCPA.*

36 Regulations § 999.313(d)(6)(c).

a company were to refuse to delete transaction records on grounds that they were required for potential litigation, the company could only use those records for litigation.

This rule would put rights-response documentation at a premium. If companies can only use retained data for statutory-exemption purposes, companies would need to document all statutory exemptions that justify retaining consumer data. Additionally, this rule could potentially test the strength of data governance structures across organizations.

Service Providers – Data Use Restrictions

21. Service providers that pool customer data to perform their services would have regulatory challenges under the Regulation.

It is not uncommon for companies to develop one-to-many platforms that commonly service a number of customers. Under the GDPR, such companies often took the position of a "data processor," and it can be expected that a number of them will take a position as a "service provider" under the CCPA. For some of these service providers, their services rely on pooling the data of their various customers to generate service models that benefit all customers.

The Regulations, in their current form, would make that kind of business model more difficult. They state that service providers "shall not use personal information received either from a person or entity it services … for the purpose of providing services to another person or entity." The only exception to this rule is that customer data can be pooled to "detect data security incidents" or "protect against fraudulent or illegal activity,"[37] possibly in recognition of the fact that such services cannot be performed without pooling significant quantities of data to detect suspicious incidents.

It is difficult to determine in advance all industries potentially affected by this portion of the Regulations, or to determine who the primary target is. Platforms that offer their customers logically separated storage and complete data ownership may not face issues. But services that use cross-customer data to provide services would presumably be potentially affected.

Alston & Bird is closely following the development of the CCPA and its Regulations. For more information, contact Jim Harvey, David Keating, Amy Mushahwar, Karen Sanzaro, or Daniel Felz.

---

[37] Regulations § 999.314(c).

You can subscribe to future *Privacy & Data Security* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Data Security Group

James A. Harvey
404.881.7328
jim.harvey@alston.com

David C. Keating
404.881.7355
202.239.3921
david.keating@alston.com

Kelley Connolly Barnaby
202.239.3687
kelley.barnaby@alston.com

Chris Baugher
404.881.7261
chris.baugher@alston.com

Kristine McAlister Brown
404.881.7584
kristy.brown@alston.com

Angela T. Burnette
404.881.7665
angie.burnette@alston.com

David Carpenter
404.881.7881
david.carpenter@alston.com

Lisa H. Cassilly
404.881.7945
212.905.9155
lisa.cassilly@alston.com

Helen Christakos
650.838.2091
helen.christakos@alston.com

Cari K. Dawson
404.881.7766
cari.dawson@alston.com

Derin B. Dickerson
404.881.7454
derin.dickerson@alston.com

Clare H. Draper IV
404.881.7191
clare.draper@alston.com

Christina Hull Eikhoff
404.881.4496
christy.eikhoff@alston.com

Sarah Ernst
404.881.4940
sarah.ernst@alston.com

Peter K. Floyd
404.881.4510
peter.floyd@alston.com

Daniel Gerst
213.576.2528
daniel.gerst@alston.com

Jonathan M. Gordon
213.576.1165
jonathan.gordon@alston.com

Elizabeth Helmer
404.881.4724
elizabeth.helmer@alston.com

John R. Hickman
404.881.7885
john.hickman@alston.com

Donald Houser
404.881.4749
donald.houser@alston.com

Stephanie A. Jones
213.576.1136
stephanie.jones@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

W. Scott Kitchens
404.881.4955
scott.kitchens@alston.com

John L. Latham
404.881.7915
john.latham@alston.com

Dawnmarie R. Matlock
404.881.4253
dawnmarie.matlock@alston.com

Amy Mushahwar
202.239.3791
amy.mushahwar@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Cara M. Peterman
404.881.7176
cara.peterman@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

Karen M. Sanzaro
202.239.3719
karen.sanzaro@alston.com

Jessica C. Smith
213.576.1062
jessica.smith@alston.com

Lawrence R. Sommerfeld
404.881.7455
larry.sommerfeld@alston.com

Peter Swire
240.994.4142
peter.swire@alston.com

Daniel G. Taylor
404.881.7567
dan.taylor@alston.com

Katherine M. Wallace
404.881.4706
katherine.wallace@alston.com

Richard R. Willis
+32.2.550.3700
richard.willis@alston.com

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ALSTON & BIRD

WWW.ALSTON.COM