ALSTON & BIRD

CCPA Privacy Briefing:
Review of Modified Proposed CCPA Regulations

February 13, 2020

The Updated CCPA Regulations: 30 Potentially Material Business Impacts

by Daniel Felz, Kathleen Benway, David Keating, and Amy Mushahwar

* * * * * *

On February 7, and February 10, 2020, California Attorney General Xavier Becerra released modified Proposed Regulations (the "Updated Regulations") for the California Consumer Privacy Act ("CCPA"). The Updated Regulations contain a number of material modifications to the initial October 2019 draft CCPA regulations released by the Attorney General's Office (the "AG's Office"). This Advisory summarizes the potentially material changes that the AG's Office has introduced in the Updated Regulations.

I. Background

On October 10, 2019, California Attorney General Xavier Becerra released Proposed Regulations (the "Regulations") for the CCPA. The Regulations contained 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. For a quick refresher on the initial October 2019 Regulations as the background for these modifications, see our list of the 21 potentially most material impacts of the original draft Regulations.

The Attorney General's Regulations generated significant interest and resulted in thousands of pages of public comments to the AG's Office. The Attorney General also held a series of public hearings at which members of the public provided feedback directly to members of the AG's Office.

The Updated Regulations respond to a number of key issues raised during the public comment period. This Advisory summarizes the modifications introduced by the Updated Regulations that are likely of material interest across industries. Note that companies have until **February 25, 2020** to submit comments on the Updated Regulations to the Attorney General. Issues covered by this Advisory are arranged by (a) Notice, (b) Rights Requests Generally, (c) Opt-Outs, (d) Deletion, (e) Access, (f) Service Providers, (g) Children's Data, (h) Financial Incentives, and (i) the Concept of Personal Data.

II. Summary of the Updated Regulations

Notice: "Notices at Collection," "Just-in-Time Notices," and the Online Privacy Policy

1. **Unchanged: "Notices of Collection" are still required over and above the Online Privacy Policy.** The original draft of the Regulations emphasized a key distinction between two types of notice the CCPA requires companies to provide: (a) a notice given by the company to the consumer precisely at the "point of collection" alerting the consumer that personal information is being collected (required under § 100(b) CCPA, which we refer to the "Notice of Collection"); and (b) a comprehensive privacy policy posted within the company's website or mobile app (required under § 135(a)(5) CCPA, which we refer to as the "Online Privacy Policy").

   The Updated Regulations maintain this distinction and continue to require Notices at Collection in addition to an Online Privacy Policy.[1] Thus, simply having an Online Privacy Policy posted on their websites remains insufficient to satisfy companies' notice responsibilities under the Regulations in many cases. Instead, in addition to having an Online Privacy Policy, companies must provide additional Notices of Collection at every specific data collection point – or forgo collecting data there entirely.[2] Following the CCPA's January 1, 2020 effective date, this aspect of the Regulations has resulted in discussion as to whether websites and mobile apps are compliant if they simply have a link to their Online Privacy Policy on their homepage footer (and/or navigation menu), or whether an additional "Notice of Collection" link is needed. Questions have further been raised as to whether the Notice of Collection can be delivered via a footer/hamburger menu link, or whether a banner- or splash-screen-style notice is needed to alert users that data is being collected as of the moment they land on the site and/or open the app.

2. **Guidance on how Notices at Collection can be delivered.** Many companies have already started displaying or linking their Notices of Collection at the points where they collect data from consumers. This often gives rise to questions of, e.g., "How early in a consumer interaction do we need to provide notice for it to be 'at or before' the point of collection?", and "How do we need to deliver the notice?" The AG's Office now provides two helpful indications of how companies can deploy Notices of Collection:
   - For mobile apps, Notices of Collection can be provided by (a) linking to the Notice in the App Store / Google Play Store download page and (b) placing the Notice in the

[1] See Updated Regulations § 999.304 (providing an overview of required notices).

[2] Updated Regulations § 999.305(a)(7).

app's navigation menu.[3] This could potentially mean that app publishers need to develop a Notice of Collection separate from their full Privacy Policy for placement in the App Store / Play Store, or that a separate link to the California content of the Privacy Policy is required.

- For telephonic interactions (such as customer support or other call centers), Notice of Collection may be given "orally."[4]

3. **The "Just-in-Time Notice" for unexpected data collection.** The Updated Regulations add a third type of notice obligations to the Notice of Collection and Online Privacy Policy: the "Just-In-Time Notice." Consistent with federal guidance, a Just-In-Time Notice must be given whenever "a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect."[5] As an example, the Updated Regulation state that if a "flashlight" app (i.e. an app that activates the flashlight function of a phone) starts collecting geolocation information, a Just-In-Time Notice is required.[6]

   The "Just-In-Time Notice" rule raises scoping and practical questions. For instance, it is currently limited to instances where data is collected from "mobile devices," but significant data can be collected from, e.g., desktop computers, smart TVs, or any other connected devices. Additionally, it is unclear whether a Notice of Collection delivered when a consumer first downloads and uses an app could set the consumer's expectations such that a later, additional Just-In-Time Notice is not needed. It is further uncertain whether the operating systems for in-scope devices (such as Apple iOS or Google Android) will permit or support the number of "Just-In-Time Notices" that may be required under this new rule, given that they may impede the mobile experience.

4. **Accessibility of notices needs to be guided by industry standards.** The initial October 2019 Regulations required all forms of CCPA-required notice to be "accessible to consumers with disabilities,"[7] leading public comments to ask the AG's Office what it would consider a sufficiently "accessible" notice to be. The Updated Regulations respond to these questions by stating that businesses "shall follow generally recognized industry standards"

[3] See Updated Regulations § 999.305(a)(3)(b).

[4] Updated Regulations § 999.305(a)(3)(d).

[5] Updated Regulations § 999.305(a)(4).

[6] Updated Regulations § 999.305(a)(4).

[7] Regulations §§ 999.305(a)(2)(d), 999.306(a)(2)(d), 999.307(a)(2(d), and 999.308(a)(2)(d).

for accessibility.[8] For online notices, the Updated Regulations indicate the AG's Office accepts the World Wide Web Consortium's Web Content Accessibility Guidelines (V2.1) as recognized industry standards.

5. **Companies' duty to include transparency statistics in their Online Privacy Policy is triggered by processing California consumer data – and now only arises when you have data of 10 million California consumers.** The initial draft of the Regulations required companies to disclose transparency statistics on their handling of CCPA requests in their Online Privacy Policy if they buy, receive, sell, or share personal information of 4 million or more consumers.[9] The statistics must show (a) the number of CCPA requests received, (b) the number of requests denied, and (c) average response times. Public comments to the AG questioned whether these transparency obligations are triggered by processing personal information relating to 4 million *California* consumers, or by processing data of 4 million consumers from anywhere.
   - The Updated Regulations now contain a distinction between "consumers" (which is defined via the CCPA as individuals residing in California) and "all individuals," an undefined term that would appear to signify natural persons both inside and outside California.[10] This suggests that transparency statistics only need to be included in Online Privacy Policies if businesses buy, receive, sell, or share personal information relating the threshold number of *California* consumers.
   - Additional revisions released by the AG's Office on February 10, 2020 raise the threshold number of California consumers to 10 million.[11] Thus, it appears companies must only include transparency statistics in the Online Privacy Policy if they buy, receive, sell, or share personal information of 10 million California consumers within a calendar year.

6. **Is there now a "*register as a data broker or email out millions of Notices of Collection*" rule?** One of GDPR's thornier notice rules is Article 14, which requires companies collecting personal information from sources other than the affected consumer to still find a way to provide privacy notices to those consumers. As the Regulations were being drafted, there was some discussion of whether they would adopt this approach to notice. The initial October 2019 draft of the Regulations expressly stated that "[a] business that does not

[8] Updated Regulations §§ 999.305(a)(2)(d), 999.306(a)(2)(d), 999.307(a)(2)(d), and 999.308(a)(2)(d).

[9] Regulations §§ 999.317(g)(1) and (2).

[10] See Updated Regulations § 999.317(g)(4) ("A business may choose to compile and disclose the information required by subsection (g)(1) for requests received from all individuals, rather than requests received from consumers.").

[11] Updated Regulations § 999.317(g).

collect information directly from consumers does not need to provide a notice at collection" if it obtains signed attestations from its data sources about the disclosures provided to consumers at the time data was collected.[12] This allayed some concern about needing to potentially mail or email millions of notices to consumers. But the attestation requirement was new to the data sourcing industry and led to questions about whether it required restructuring of industry practices.

The Updated Regulations take a different approach: Companies that collect data from sources other than the affected consumer only receive an exemption from CCPA notice obligations if they (a) "register[] … as a data broker" under California's data broker statute, and (b) make sure their California data broker registration informs consumers about how to submit Opt-Out requests.[13] Potentially, this revised approach aims to incentivize data companies to registers as data brokers. Otherwise, under the current draft of the Updated Regulations, companies that purchase, lease, or otherwise acquire data may have to deliver Notices of Collection to all the California consumers whose data they purchase or acquire, and would arguably not be permitted to use such data until appropriate Notices were provided.

7. **Employment notices can be separate from consumer notices.** Assembly Bill 25 largely exempted personal information relating to employees, contractors, and job applicants from the CCPA, with the exception that businesses must still provide Notices of Collection to such persons. The initial October 2019 Regulations did not address employment-related notices, but the Updated Regulations provide several clarifications. First, the Updated Regulations recognize that companies can have employee or applicant privacy notices separate from their consumer notices.[14] Second, employment-related notices can be provided via "a link" (such as in an online job application form) or "a paper copy" (such as in onboarding paperwork).[15] Lastly, the Updated Regulations expressly confirm that employee or applicant privacy notices do not require a Do Not Sell My Info section.[16]

Rights Requests Generally

8. **Retailers, exhale: The in-store CCPA rights request form is no longer required.** The initial October 2019 Regulations draft required companies that "primarily interact[]" with

[12] Regulations § 999.305(d)(2).

[13] Updated Regulations § 999.305(d).

[14] Updated Regulations § 999.305(e)(2).

[15] Updated Regulations § 999.305(e)(2).

[16] Updated Regulations § 999.305(e)(1).

consumers offline – such as in a retail setting – to offer in-person methods for submitting CCPA rights requests, such as paper forms.[17] Retailers across industries submitted comments on the risks of this requirement to the AG's Office, such as the risk of asking millions of store, restaurant, and similar personnel to securely handle customers' personal information and reliably transmit rights requests. The AG's Office appears to have recognized these risks, and no longer requires businesses to provide in-person methods for submitting rights requests. Instead, the Updated Regulations requests that brick-and-mortar businesses "consider" providing an in-person method for letting customers submit in-store CCPA requests.[18] They also expressly recognize as acceptable more secure and reliable methods suggested by retailers during the public comment process, such as an in-store tablet where a consumer could fill out a CCPA request form.[19]

9. **Make sure any vendors whose tools you use for CCPA compliance have clear "service provider" language.** The AG's October 2019 draft of the Regulations required companies to retain all records relating to CCPA requests for 24 months.[20] This retention period remains unchanged; however, the Updated Regulations now also state that retained CCPA request records "shall not be shared with any third party."[21] Of course, many companies use compliance and/or IT ticketing vendors to help them manage CCPA records. To ensure these vendors are compliant with the Updated Regulations, appropriate contractual terms should be in place so that the vendor is a "service provider" and not a "third party" as defined in the CCPA.

10. **Identity verification for CCPA rights requests cannot result in costs to consumers.** The Updated Regulations largely maintain the ID verification requirements contained in the AG Office's initial October 2019 draft of the Regulations. However, the Updated Regulations add that businesses cannot "require the consumer to pay a fee" for ID verification.[22] The Updated Regulations appear to interpret the concept of "fee" broadly, stating that "a business may not require a consumer to provide a notarized affidavit" as part of ID verification unless they "compensate the consumer for the cost of

[17] Regulations § 999.312(c)(2).

[18] Updated Regulations § 999.312(c).

[19] Updated Regulations § 999.312(c).

[20] Regulations § 999.317(b).

[21] Updated Regulations § 999.317(e).

[22] Updated Regulations § 999.323(d).

notarization."[23] This indicates that ID verification procedures cannot result in costs to consumers.

11. **You do not have to break the law to explain why you denied a CCPA request.** Both the original 2019 Regulations and the Updated Regulations require companies that deny a CCPA request in whole or in part to describe the basis for the denial. In response to public comments, the Updated Regulations now specify that companies do not have to provide this description if prohibited by law.[24]

Opt-Out Requests

12. **Opt-Outs must be as uncomplicated as practicable.** The CCPA's statutory text does not expressly state how companies should intake Opt-Out requests. The Updated Regulations now state that Opt-Outs must "be easy for consumers to execute" and must "require minimal steps."[25] Businesses cannot use methods that are intended to, or have the "substantial effect," of "subverting or impairing" consumers' attempts to Opt-Out.[26] This may be a response to opt-out submission methods the AG's Office witnessed after January 1, 2020. As can be seen below, it appears consistent with an effort by the Updated Regulations to incentive instantaneous, self-serve opt-out methods.

13. **Do Not Track is still back - but the signals for a "CCPA DNT" might still need to be developed.** The initial October 2019 draft of the Regulations garnered attention by requiring companies to treat "user-enabled privacy controls" like browser settings as Opt-Outs for the user's Internet browser or device.[27] This seemed to resemble a requirement to treat Do Not Track signals as Do Not Sell requests, even though an industry standard for Do Not Track does not yet exist despite years of discussion.

    The Updated Regulations have maintained the requirement to treat DNT-like signals as Do Not Sell requests, but appears to recognize that technical work will need to be done before this rule can be operationalized. Signals from user privacy controls must "clearly communicate that a consumer intends to opt-out of the sale of personal information"

[23] Updated Regulations § 999.323(d).

[24] Updated Regulations §§ 999.313(c)(5) and (d)(6)(a).

[25] Updated Regulations § 999.315(c).

[26] Updated Regulations § 999.315(c).

[27] Regulations § 999.315(g).

before they must be treated as Do Not Sell requests[28] – and it is unclear whether any such controls presently exist. Further, privacy controls cannot have "pre-selected settings;" instead, they must require consumers to "affirmatively select their choice to opt-out."[29] They must also be "global",[30] so, e.g., an opt-out cookie placed in a user's browser by one website's cookie management tool may not amount to a Do-Not-Sell signal for other websites. On the whole, it appears the AG's Office may be inviting the development DNT technology aimed towards broadcasting CCPA Do-Not-Sell signals.

14. **The 90-day look-back for Do-Not-Sell requests is gone – but the AG's Office is now incentivizing instantaneous Opt-Out methods.** The October 2019 draft of the Regulations contained a 90-day look-back: Companies that received an Opt-Out needed to identify all the businesses to whom they had sold the requestor's data in the prior 90 days, then contact those businesses and instruct them to stop selling that individual's data.[31] The prospect of needing to log all data sharing that amounts to a CCPA "sale" caused significant IT discussions throughout organizations of all sizes. The Updated Regulations have done away with the 90-day look-back requirement – likely providing significant relief to many companies. However, they still require companies to flow-down Do-Not-Sell requests to the recipients of any data "sales" that occur between (a) the time where the consumer submits an Opt-Out request, and (b) the time at which the request is executed.[32] This appears to incentivize one-click Opt-Out buttons, preference management solutions, or similar consumer self-serve mechanisms that result in the instantaneous execution of an Opt-Out request.

15. **Service providers must respect Opt-Outs received by the businesses they serve.** Neither the CCPA's statutory text nor the October 2019 draft of the Regulations addressed whether service providers had to assist businesses they serve in the execution of Opt-Outs. The Updated Regulations now state that service providers "shall not sell data on behalf of a business" they serve when "a consumer has opted-out of the sale of their personal information with the business."[33] This may be directed at intermediaries in the adtech space that share data as part of performing their services, but do so on behalf of their customers.

---

[28] Updated Regulations § 999.315(d)(1).

[29] Updated Regulations § 999.315(d)(1).

[30] Updated Regulations § 999.315(e).

[31] Regulations § 999.315(f).

[32] Updated Regulations § 999.315(f).

[33] Updated Regulations § 999.314(d).

16. **You still can't sell data you collected before you posted a "Do Not Sell My Info" link**. Under the original October 2019 draft of the Regulations, if a business collected personal information without posting a "Do Not Sell My Info" link, all individuals whose data the business collected were automatically deemed to have made a Do-Not-Sell request.[34] The Updated Regulations now no longer contain an "Opt-Out-by-operation-of-law" for such situations. But they still prohibit the business from selling personal information collected before the "Do Not Sell My Info" link was posted until it obtains "affirmative authorization" from the affected consumers, e.g. via an opt-in.[35] This rule may seek to incentivize businesses who are on the fence about whether they "sell" data to post a Do Not Sell My Info link.

Deletion Requests

17. **Double-opt-in for Deletion requests is no longer mandatory.** Businesses no longer "must" use a two-step process for confirming that a consumer wishes to delete her data. Instead, under the Updated Regulations they "may" use such a process.[36]

18. **Unverifiable Deletion requests no longer need to be automatically converted into Opt-Out requests – but consumers still need to be asked if they want to Opt-Out.** Under the October 2019 draft of the Regulations, if a Deletion request was denied because the requestor's identity could not be verified, the business was required to treat it as a Do Not Sell request.[37] Public comments took issue with the ability to comply with this requirement in practice. The Updated Regulations now no longer require unverifiable Deletion requests to be converted into Opt-Outs. Instead, businesses must notify the consumer that the Deletion request has been denied and ask the consumer if she would like to Opt-Out.[38]

19. **Suppression files appear to be permitted to support forward-looking deletion.** One issue companies can face in building Deletion workflows is that at times, a "suppression file" containing the deleted individual's name must be maintained so that the company can prevent re-ingestion of that individual's data into its systems. The suppression file thus helps companies "remember they forgot" individuals who have requested deletion. The Updated Regulations now permit businesses to "retain a record of" Deletion requests to

[34] Regulations § 999.306(d)(2).

[35] Updated Regulations § 999.306(e).

[36] Updated Regulations § 999.312(d).

[37] Regulations § 999.313(d)(1).

[38] Updated Regulations § 999.313(d)(1).

ensure that "the consumer's personal information remains deleted from the business's records."[39]

Access Requests

20. **ID verification in the Access context is important – you must deny Access requests if you cannot verify requestor's ID.** For Deletion and Opt-Out requests, the Updated Regulations contain rules stating when a business "may" deny the request.[40] Not so for Access requests, potentially recognizing the heightened risk presented when a business hands over its comprehensive data set about an individual to a person claiming to be him or her. Thus, the Updated Regulations state that if a business "cannot verify the identity of the requestor" as required under the Regulations, it "must" deny an Access request.[41]

21. **Companies do not have to provide "household" information in response to Access requests unless the whole household asks for it and is verified.** Personal information is defined by the CCPA as any information relating to a "household,"[42] but during public comment risks surrounding the disclosure of "household" data were raised – such as whether it is safe to hand data relating to an entire household to one person purporting to be a member of the household. The Updated Regulations now contain more detailed regulations for verification of Access requests relating to household data. If a household lacks a password-protected account with a business, businesses do not need to provide household data to a requestor unless (a) all members of the household jointly make the request, (b) each household member's ID is verified, and (c) each requestor is verified to be a current member of the household.[43] If a business has a password-protected account with a household, it may follow its "existing business practices" to "process" Access requests relating to household data to the extent they are "in compliance with" the Updated Regulations.[44]

22. **Biometric data is now on the never-to-be-disclosed list.** The October 2019 draft of the Regulations contained a list of types of data that companies were never permitted to disclose in response to an Access request, such as social security numbers, financial

[39] Updated Regulations § 999.313(d)(5).

[40] Updated Regulations §§ 999.313(b), 999.313(d)(1), 999.315(g), and 999.315(h).

[41] Updated Regulations §§ 999.313(b) and 999.325(f).

[42] § 1798.140(o)(1) CCPA.

[43] Updated Regulations § 999.318(a),

[44] Updated Regulations § 999.318(b),

account numbers, or account passwords.[45] The Updated Regulations add two additional types of data to the do-not-disclose list: "unique biometric data generated from measurements," and "technical analysis of human characteristics."[46]

23. **Archives now appear to be out-of-scope for Access requests.** The Updated Regulations state that a business that receives an Access request is not required to search for personal information in systems where the personal information (a) is not maintained in searchable or readily accessible form, (b) is maintained "solely for legal or compliance purposes," and (c) is not sold or used for commercial purposes.[47] This reads like language used in some national GDPR implementation statutes meant to exempt archived records from Access requests.

Service Providers

24. **Service providers are no longer prohibited from pooling customer data to provide services to many customers.** One of the more discussed rules of the October 2019 draft of the Regulations was a prohibition on service providers from using data received from providing services to one of its customers to support the services it provided to its other customers.[48] This rule potentially affected the business models of a broad number of industries, such as, for instance, shipping, transportation, or logistics providers. Several comments were submitted to the AG's Office warning of unanticipated affects of this rule on key U.S. industries. The Updated Regulations now no longer contain a rule that prohibits service providers from pooling customer data to support the services they offer to all customers. Instead, service providers are merely limited to using customer data to "perform the services specified in the written contract" with "the business that provided" the data.[49] This may put a premium on agreeing to fairly uniform service descriptions across customers.

25. **Service providers can use customer data for internal R&D, if this does not venture into high-risk use cases.** The Updated Regulations also expressly provide that service providers can use customer-provided personal information for "internal use … to build or improve the quality of its services."[50] However, internal R&D with customer information

[45] Regulations § 999.313(c)(4),

[46] Updated Regulations § 999.313(c)(4),

[47] Updated Regulations § 999.313(c)(3),

[48] See Regulations § 999.314(c),

[49] Updated Regulations § 999.314(c)(1),

[50] Updated Regulations § 999.314(c)(3),

may not venture into "building or modifying household or consumer profiles," or "cleaning or augmenting data acquired from another source."[51]

Children's Data

26. **Companies need a documented process for verifying the ID of parents & guardians who submit CCPA requests on behalf of their children.** The Updated Regulations require business who hold data of children under 13 to "establish, document and comply with" a method for verifying that a person submitting an Access or Deletion request on behalf of a child "is the parent or guardian of that child."[52] The creation of these types of ID verification policies, and their associated Access and Deletion workflows, could have COPPA implications that must be addressed in parallel. If companies believe these issues could use further clarification, the remaining comment period would be a suitable time to bring them to the attention of the AG's Office.

Financial Incentive and Loyalty programs

27. **If you can't calculate the value of consumer data, you can't offer a financial incentive program.** For businesses that offer financial incentive programs, the October 2019 draft of the Regulations introduced a requirement to calculate a good-faith estimate of the value of consumers' data.[53] This led to many public comments relating to the lack of any commonly-accepted methods for arriving at a valuation of consumer data. Nonetheless, the AG's Office has re-emphasized the importance of calculating the value of consumer data as a basis for financial incentive programs. The Updated Regulations now state that "[i]f a business is unable to calculate a good-faith estimate of the value of the consumer's data …, that business shall not offer the financial incentive."[54] (Still, in response to some public comments, the AG has clarified that in calculating the value of consumer data, businesses do not need to rely exclusively on the value of data relating to *California* consumers.)[55]

28. **For organizations with loyalty programs: You do not have to delete rewards data about individuals who want to stay part of the loyalty program.** The Updated Regulations allay some concerns of retailers about being held to discriminate against loyalty program

[51] Updated Regulations § 999.314(c)(3),

[52] Updated Regulations § 999.330(c),

[53] Regulations § 999.337(a),

[54] Updated Regulations § 999.336(b),

[55] Updated Regulations § 999.337(b),

members by either deleting their data in response to a Deletion request (and thus eliminating earned rewards), or by not deleting their data (and thus allegedly treating them differently than non-loyalty members). The Updated Regulations now state in a case example that if a consumer "submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program," the business does not need to delete the data that is necessary to provide the loyalty program to the consumer.[56]

29. **But be careful in executing CCPA requests if that removes consumers from loyalty programs or blocks loyalty rewards – you can do that only if you have documented that executing the CCPA request causes a comparable loss to you because you must delete (or may no longer sell) consumer data.** The Updated Regulations provide further examples of when deletion or opt-outs that eliminate consumers' loyalty program participation or earned rewards are permissible. For example, grocery stores' loyalty programs may depend on sharing data with third-party food manufacturers, meaning that an opt-out hinders the ability to provide the consumer with coupons and special discounts. If a consumer requests an Opt-Out, the grocery store may only remove the consumer from the loyalty program it "can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business."[57] In other words, the business must document in advance that the "loss" the business will incur by not being able to sell the consumer's data is reasonably related to the "loss" the consumer will incur by not receiving coupons and special discounts.

30. **Publisher business models may be captured by the above nondiscrimination rules.** Some publisher platforms offer paid subscriptions alongside "free" offerings that are financed by online advertising. The Updated Regulations make clear that the above rules apply to these types of business models as well. As an example, the Updated Regulations name a music streaming service that offers a $5-per-month premium subscription and a "free" model. The streaming platform cannot stop the "free" users from opting-out of data sales unless it demonstrates that the "loss" it would suffer from not being able to sell free users' data is reasonably related to the $5 the users would otherwise have to pay to opt-out.[58] This interpretation of CCPA nondiscrimination rules may put a premium for publishers and their vendors to quantify users' value across their platforms. This may be challenging in an environment where different positions are being taken as to what kinds of digital analytics and online advertising arrangements rise to the level of a CCPA "sale." More

[56] Updated Regulations § 999.336(d)(2),

[57] Updated Regulations § 999.336(d)(3),

[58] Updated Regulations § 999.336(d)(1),

fundamentally, however, the Updated Regulations appear to indicate that the AG's Office is viewing common publisher business models that distinguish between "free" and tiers of paid access to content through the lens of "financial incentive programs" and non-discrimination rules.

What is "Personal Information" for CCPA Purposes?
(Or: Did the AG's Office Just Create a Carve-Out for Online Advertising?)

31. **The AG's Office may be signaling it will interpret the concept of "personal information" pragmatically, but companies should still be wary of a broad concept of data "sales."** The Updated Regulations begin with new "guidance" about what should – and should not – be considered "personal information." The Updated Regulations state that the test is "whether the business maintains information in a manner" that identifies, is reasonably capable of being associated with, or could be reasonably linked to, a consumer. As an example, if a business collects IP addresses from visitors to its website, but "could not reasonably link the IP address with a particular consumer or household," the IP address is not personal information.[59]

- This guidance likely responds to questions about the scope of "personal information" raised by a number of companies and industry associations during public comment. Businesses expressed concern that they could be held in violation of the CCPA for not producing or deleting certain types of non-identified data in response to consumer CCPA requests, because – even though the business had no way to link that information to a consumer on its own – someone somewhere could potentially make the link, thus making the data "personal information" under the CCPA. European Court of Justice decisions holding that dynamic IP addresses constitute "personal data" under the GDPR likely played a role in these discussions.

- Still, the Updated Regulations' new "guidance" on the concept of personal information seems to raise as many questions as it answers. First, it is unclear how much effort the AG's Office considers "reasonable" in determining whether a business could "reasonably link" data to an individual or household. For example, a business may have four separate data repositories that are not linked, run on different database software, and two are in the cloud. But, if a query could be run across all of them, the business could determine whether it has an identifiable record that could be linked to an IP address from its web server logs. How much work does a business need to do to have "reasonably" attempted to find all "linkable" data in its enterprise? Industry is likely to take a spectrum of views as to what is "reasonable."

[59] Updated Regulations § 999.302(a),

- More importantly, the new "guidance" raises question as to whether the AG's Office is creating a CCPA carve-out of online advertising and digital analytics from CCPA "sales" rules. Through these activities, many businesses end up holding data that they themselves cannot link to any individual – but which they share with analytics and advertising partners who can. These sharing arrangements often stand in the middle of the debate about what constitutes a "sale" of personal information.

  For example, many businesses have integrated cookies, pixels, software development kits, and similar tracking technologies into their websites and mobile apps. These technologies output site interaction data tied to a cookie or similar persistent but random ID. The business operating the website/app often cannot link a cookie ID to a consumer. But, cookie data is shared with vendors who can tie the cookie ID to a known consumer, household, or device. If the business could never link cookie data with an individual on its own, it is arguably not "personal information" under the Updated Regulations' new guidance – so if the business transfers that cookie data to an adtech vendor, the business now appears to have a position that it has not shared any "personal information," even if the adtech vendor can link the cookie data to an individual or device on its end.

  But that is exactly how much of online advertising and digital analytics work – businesses provide adtech partners with data the business cannot itself link, but which it hopes the vendor can link to enable targeting, ID graphing, measurement, and other advertising use cases. Thus, the Updated Regulations' new guidance, read broadly, would potentially enable businesses to argue that their online advertising and digital analytics activities are <u>not</u> CCPA sales (and are further not subject to the CCPA, since the business itself cannot associate adtech-related data with individuals).

  It is not clear that the AG's Office intended for its new "guidance" to create such a restrictive reading of the term "personal information" that would enable this result. Companies should thus be cautious in taking any position that the Updated Regulations change their CCPA obligations in regard to digital analytics and online advertising.

- Potentially, the AG's Office is seeking to limit the burden on businesses who are building the processes by which they search their organization to produce information in response to Access requests. For that case, the Updated Regulations' guidance on what should be pulled into the response as "personal information" are potentially helpful. For other cases – and particularly for data sharing that risks being a CCPA

"sale" – it may still be risky for companies to adopt a restrictive reading of "personal information."

Privacy Briefing Authors

VIEW FULL BIOGRAPHY

Daniel J. Felz – Senior Associate

Dan leverages his extensive international experience to advise clients on global privacy, cybersecurity, technology, and adversarial matters. After graduating Order of the Coif from law school, Dan was an assistant professor of law at the University of Mainz School of Law in Germany. Dan clerked for the U.S. District Court for the Southern District of Georgia, the 68th Judicial District Court of Dallas County, and the U.S. District Court for the Northern District of Texas.

Contact: daniel.felz@alston.com | 404.881.7694

VIEW FULL BIOGRAPHY

Kathleen Benway – Partner

Drawing on more than 12 years of service at the FTC, including most recently as chief of staff for the agency's Bureau of Consumer Protection, Kathleen brings significant regulatory, legislative, and enforcement experience in consumer protection law, including in privacy, data security, and advertising. Kathleen concentrates her practice on government investigations and corporate compliance, and also supports clients in policy and rulemaking proceedings tied to the CCPA, COPPA, and GLB Safeguards Rule.

Contact: kathleen.benway@alston.com | 202.239.3034

VIEW FULL BIOGRAPHY

David C. Keating – Partner

David focuses his practice on matters involving technology and data and co-leads the Privacy & Data Security Team. He has advised clients on privacy and security issues arising along the entire data life cycle for 20 years. He has significant experience with new and emerging data protection laws, including the California Consumer Privacy Act and the EU General Data Protection Regulation.

Contact: david.keating@alston.com | 404.881.7355

VIEW FULL BIOGRAPHY

Amy S. Mushahwar – Partner

Amy provides advice to clients on proactive data security practices, data breach incident response, emerging technology (such as, loT, Big Data, cloud computing, AdTech, FinTech, and artificial intelligence), and regulatory compliance. Having been a former technology consultant and chief information officer (CISO), Amy frequently advises businesses on the practical impact of new technology.

Contact: amy.mushahwar@alston.com | 202.239.3791