CCPA Implementation: An Early Map

Alysa Z. Hutnik, Aaron J. Burstein, Alexander I. Schneider

January 7, 2020

The January 1, 2020 effective date of the California Consumer Privacy Act (CCPA) has come and gone, but questions about how to comply with the law show no hint of disappearing. As companies move past their efforts to comply with the law's most visible requirement – providing notice at the point of collection and explaining data practices in a full privacy policy – the focus is sharpening on a broad array of operational and implementation questions.

While Attorney General Xavier Becerra has indicated his office will prioritize enforcement relating to the sale of minors' personal information, will direct enforcement efforts at companies that are not showing a willingness to comply, and will not make major changes before finalizing the proposed regulations, the Attorney General has not fielded specific questions about how to implement the law. This state of affairs has left companies scrambling to benchmark their compliance practices against competitors and the industry at large.

In this post, we provide some insights on common questions we are hearing about how to comply with the CCPA in the absence of clear guidance or precedent. Of course, every company is different and companies should always consult with a privacy attorney before deciding on the best way to comply with the CCPA.

- **Why are so many companies posting a "Do Not Sell My Info" (DNSMI) button on their website if they do not sell personal information in exchange for money?**
- **When can a business claim that its ad tech partner and purchased ad tech services are exempt from the "sale" provisions of the CCPA?**
- **What are the IAB and DAA options for ad tech compliance?**

- **How do privacy technology vendor tools factor into CCPA Do Not Sell compliance?**
- **What best practices can companies adopt when verifying a consumer request before providing personal information to the requestor?**
- **Where are companies posting their DNSMI links?**
- **What should we do when a consumer clicks on our DNSMI link?**
- **What does the B2B exemption mean?**
- **We're a business, and we sell personal information. Do we have to pass through consumer requests to entities to which we sold data?**
- **Is there a potential for a private right of action for privacy issues?**
- **What's happening with California's *new* privacy ballot initiative?**

Why are so many companies posting a "Do Not Sell My Info" (DNSMI) button on their website if they do not sell personal information in exchange for money?

Companies that post a DNSMI button but do not sell personal information for money likely have determined that their provision of personal information to ad tech companies in connection with interest-based advertising is a "sale." Accordingly, they post the DNSMI button to enable consumers to opt out of these "sales."

The question of whether, and under what circumstances, the use of third-party cookies, pixels, tags, etc. constitutes a "sale" and how to provide DNSMI choices is a flashpoint in the debate over how to interpret the CCPA (as discussed here, here, and here). There is a growing consensus that only a lawsuit or a government enforcement action will resolve this matter.

For now, two ways of analyzing this question are emerging. One position concludes that data collected via a third-party cookie, tag, or pixel may be a potential "sale" because the company adding that cookie, tag, or pixel to its website sends, makes available, or otherwise shares personal information to an ad tech provider in exchange for services, and, critically, where that provider does not restrict its use or sharing of that personal information for the provider's or other entities' commercial benefit (other than for a limited number of exempted purposes).

The other position is that the third party directly collects personal information via the cookie, tag, or pixel placed on a publisher's website, and the publisher is not selling that personal information to the third party responsible for the tracker.

Each business, however, will need to evaluate, on a case-by-case basis, whether its interest-based advertising, analytics, and other forms of tracking may constitute a sale under the CCPA. Often this starts with categorizing the types of vendors and partners (i.e. ad tech, analytics, or other services); identifying each specific vendor or partner responsible for the tracker on the business's site(s); and reviewing the vendor or provider's publicly posted terms, privacy policy, and contract with the business, if there is one, to determine if the transfer of personal information to the vendor could reasonably qualify as a transfer for a business purpose to a service provider, or other exemption, or whether the transfer is likely a "sale."

When can a business claim that its ad tech partner and purchased ad tech services are exempt from the "sale" provisions of the CCPA?

The CCPA provides an exemption from the definition of a "sale" when a business uses or shares with a "service provider" personal information of a consumer that is necessary and proportionate to perform a "business purpose." As a result, companies may want to determine (1) whether an ad tech vendor is a "service provider" and (2) whether that vendor performs its ad tech service for a "business purpose." Examining specific arrangements with each advertising partner is the best way to address this question and for each of the relevant services provided by the vendor.

Some of the major players in online advertising have laid down public markers that can be helpful in classifying interest-based advertising activities. Examples include:

- Google asserts that "we never sell personal information" and provides advertisers and publishers with an array of "restricted data processing" options. Essentially, these options allow businesses that use Google for advertising to tell Google to handle personal information as a service provider, i.e., to use the information only for ad delivery, reporting, and measurement; to detect security incidents and prevent fraud; and for a handful of other specific purposes. Businesses will need to determine if restricted data processing is on by default or should be activated for the Google services they use.
- Facebook likewise asserts that "we don't sell your personal data to advertisers." Facebook has also released California-specific terms that track the CCPA's service provider structure. However, it does not appear that Facebook has incorporated these provisions into the terms that govern the use of its products.
- Twitter offers a new Data Processing Addendum specifically tailored to identify Twitter as a "service provider" under CCPA, and answers CCPA-related FAQs on its privacy portal. For companies using Twitter's advertising pixel, Twitter says it is a "business with respect to personal information it receives through the Twitter pixel."
- LinkedIn affirms that it does "not sell your personal information" and adds that "we do not sell personal information, so we don't have an opt out." LinkedIn has not provided its view on whether it is a "service provider" with respect to its advertising services.
- Two major digital advertising industry groups – the Digital Advertising Alliance (DAA) and the Interactive Advertising Bureau (IAB) have introduced their own CCPA frameworks. We discuss these two frameworks below.

What are the IAB and DAA options for ad tech compliance?

The Direct Advertising Alliance (DAA) and the Interactive Advertising Bureau (IAB) have set forth two quite different frameworks to address interest-based advertising issues under the CCPA.

- IAB's CCPA Compliance Framework for Publishers & Technology Companies consists of contractual and technical elements that allow online advertising market participants to communicate and respond to Do Not Sell requests. This is a voluntary self-regulatory framework that, in essence, allows participating publishers to tell ad tech providers that a particular consumer has opted out of sale, and that they must not sell that consumer's personal information. Think of an opt-out request as triggering a cascade of communication from the publisher to downstream ad tech providers, instructing them not to sell personal information of the opted-out consumer. The Framework, however, allows these downstream entities to use personal information in limited ways that are consistent with the "business purpose" use limitations on service providers under the CCPA.

- DAA's CCPA Opt-Out Tools follow the approach of DAA's existing YourAdChoices icon. In DAA's CCPA-specific framework, publishers may license a separate icon and use it to direct consumers to a DAA-administered page that allows consumers to opt out of sale by participating ad tech companies. In contrast to the IAB Framework, DAA's approach does not depend on Do Not Sell signals to be transmitted by a publisher to its ad tech providers. Instead, consumers ultimately tell participating ad tech providers directly that they do not want their personal information to be sold.

Companies can determine whether to participate in one or both frameworks based on a review of their position in the ad tech ecosystem, use of ad tech, compliance resources, and risk profile.

How do privacy technology vendor tools factor into CCPA Do Not Sell compliance?

Privacy technology vendors like OneTrust, Clarip, and Truyo have assisted companies with the backend technology needed to fulfill CCPA rights requests. In a Do Not Sell context, these tools can leave cookies on a consumer's device indicating that the consumer has opted out of the sale of their personal information. Some tools can turn off only cookies associated with the "sale" of personal information, sparing cookies associated with vendors classified as "service providers," uses that are classified as "business purposes," and functions that are necessary to offer a service to the consumer.

Adopting a vendor-based compliance solution typically involves a substantial investment, and it can be difficult to unwind or migrate to a different vendor. Resources like the IAPP's annual privacy tech vendor report and consultations with a privacy attorney can help companies determine whether a vendor-based solution – and which one – is right for them.

What best practices can companies adopt when verifying a consumer request before providing personal information to the requestor?

In the interim period before the publication of final regulations, businesses can use the processes set out in the draft regulations for verifying consumer requests.

Businesses are only required to respond to access or deletion requests that are verified. Two guiding principles emerged from the CCPA regulations that the California Attorney General's Office proposed in October: (1) responding to consumer requests entails some risk for businesses and consumers, and verification procedures should take these risks into account; and (2) businesses should strive to use personal information that they already have – rather than collecting additional information – to verify consumers. As a result, companies can tailor their verification processes to be consistent with the types of personal information collected and their relationships with end consumers. Note that there is not an affirmative legal requirement for businesses to verify that a consumer is a California resident to take advantage of the rights in the CCPA.

Some companies' verification disclosures reflect these principles. For example, Apple advises non-account holders that it may ask requestors for information including "name, contact information, and information related to your transaction or relationship with Apple, but the specific information requested may differ depending on the circumstances of your request for your security and to protect privacy rights."

Where are companies posting their DNSMI links?

A survey of websites indicates that companies are posting the DNSMI link on every web page in the footer area of the page. The CCPA requires businesses that sell personal information to post clear

and conspicuous DNSMI links on “any internet web page where personal information is collected.” Many companies interpret this directive to mean that a business that sells personal information must post a DNSMI on every web page. The CCPA is otherwise silent as to where the DNSMI link must be located.

What should we do when a consumer clicks on our DNSMI link?

Under the CCPA, the DNSMI link must take consumers to a webpage that enables them to opt out of the sale of their personal information. The opt-out must be effective for at least 12 months, and businesses must not use personal information that they collect in connection with taking in opt-out requests for any purpose other than fulfilling the request.

One of the questions that the CCPA leaves open is whether an opt-out request must apply to all personal information a business sells. The AG’s proposed regulations answer this question by stating that businesses must provide a global opt-out option, though businesses also may offer more limited opt-out choices. Other provisions of the proposed regulations would expand and add detail to the statutory Do Not Sell requirements. Specifically, the regulations would require businesses to respond to Do Not Sell requests within 15 days of receipt, maintain at least one additional opt-out method (e.g., a toll-free phone number or a designated email address), interpret browser-based privacy controls as opt-out signals, and instruct all third parties to which it sold a requestor’s personal information in the 90 days before receiving the request to refrain from selling that consumer’s information.

What does the B2B exemption mean?

The B2B exemption (California Civil Code section 1798.145(n)) is perhaps the least clear of the CCPA amendments enacted in 2019. Given its limited legislative history and clunky construction, companies may be overlooking the benefits of the amendment.

The B2B exemption exempts a business from complying with certain provisions of the CCPA, such as the rights to access and delete personal information and the requirement to provide a DNSMI button. The exemption will expire on January 1, 2021 unless amended. The exemption applies when:

- there is a “written or verbal communication or a transaction between the business and the consumer,”
- where the consumer is a natural person acting as an employee, owner, director, officer, or contractor of a company, nonprofit, or government agency (which is not the business),
- and the consumer’s communications or transactions with the business occur solely within the context of:
    - the business conducting due diligence regarding the company, nonprofit, or government agency, or
    - the business providing or receiving a product or service to or from such company, nonprofit, or government agency.

In other words, when a representative of a company contacts a business and provides personal information to the business, the business is not required under the CCPA to respond to CCPA rights requests or have a DNSMI link with respect to that individual in his or her capacity as a representative of the company. In addition, if the personal information is provided solely within the

context of a business providing a product or service to another company, that data flow appears to be covered by this exemption (although, depending on the facts, this type of arrangement should be evaluated under the data broker definition).

For businesses operating in the B2B space, this B2B exemption is an important one. To claim the exemption, a business should document its B2B analysis identifying activities eligible for the exemption, as well as the business's procedures for handling such personal information, and closely monitor for potential new legislation that could extend (or modify) the exemption so that it does not sunset within a year.

We're a business, and we sell personal information. Do we have to pass through consumer requests to entities to which we sold data?

The CCPA does not provide a statutory requirement for businesses to pass through consumer requests to third-party buyers of personal information. However, the draft regulations propose a 90 day window during which a business must notify third party buyers of personal information that a consumer has exercised the right to opt out of the sale of personal information and to instruct the buyer not to further sell the information. We are tracking to see if this rule remains in the final regulations.

Is there a potential for a private right of action for privacy issues?

The CCPA only provides for a private right of action for data breaches; otherwise, the CCPA is seemingly explicit in stating that "[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law." However, as our firm has written previously, we expect plaintiffs to try to find ways to leverage the law's rights and compliance obligations into new legal theories. Paying close and ongoing attention to the CCPA's statutory and regulatory requirements, as well as in industry practices, will be essential to mounting a robust defense against any such claims.

What's happening with California's *new* privacy ballot initiative?

As we noted in December, the CCPA's effective date might be the midway point of the CCPA marathon. (We stand by "might" and note that the uncertainty cuts both ways.) On behalf of the organization Californians for Consumer Privacy, Alastair Mactaggart (who filed the ballot initiative that led to the enactment of the CCPA in 2018) has filed a new initiative entitled "The California Privacy Rights Act of 2020," a/k/a CCPA 2.0.

Californians for Consumer Privacy has 180 days from December 17 to gather at least 623,212 signatures (based on 5% of the total votes cast in the last gubernatorial election) to get the initiative on the November 2020 ballot. (For reference, the group had obtained 629,000 signatures by June 2018 for CCPA 1.0.)

Styled as an amendment to the CCPA, this initiative would make far-reaching changes to the current statute. Some of the most significant changes in CCPA 2.0 include:

- Imposing heightened restrictions on "cross-context behavioral advertising";
- Introducing a definition of "sensitive personal information" and imposing heightened restrictions on the use and disclosure of such information; and
- Revising the structure of business-service provider relationships; and
- Creating a dedicated state-level privacy regulatory agency.

Have other CCPA questions?

If there are other questions you’re interested in our blog covering for CCPA, feel free to send us a note.