Considerations for Digital Media Publishers and Advertisers Seeking to Engage Ad-tech Companies as CCPA "Service Providers"

September 2020

About the NAI

Founded in 2000, the Network Advertising Initiative (NAI) is the leading self-regulatory organization representing third-party digital advertising companies. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing high standards for data collection and use for digital advertising in multiple media, including web, mobile, and TV.

Acknowledgments

This document was prepared by participants in the NAI's CCPA Implementation Working Group, a joint effort consisting of leading CCPA experts from NAI member companies and the NAI staff.

Contact

Tony Ficarrotta **(**tony@networkadvertising.org**)**
Counsel, Compliance & Policy, NAI

I. Introduction

Preparations for compliance with the California Consumer Privacy Act (CCPA)[1] have been checkered with uncertainty ever since the law passed in 2018. There are many questions still left unanswered about how the CCPA and its implementing regulations will apply to the digital advertising ecosystem, even after a round of amendments to the CCPA,[2] and multiple rounds of proposed rules promulgated by the Office of the Attorney General (OAG).[3] Indeed, the CCPA's many ambiguities and uncertainties may take years of experience to resolve. Still, the fact that the CCPA and its final implementing regulations are now being enforced[4] makes this a good time for both digital media publishers and brand advertisers to evaluate how they are working with their ad-tech partners to position themselves for compliance with the CCPA.

One strategy for CCPA compliance that businesses are exploring (or are already relying on) is the use of contracts designed to make their ad-tech vendors CCPA "service providers."[5] In theory, a business's use of a service provider contract in connection with its transfer of "personal information"[6] to an ad-tech vendor would prevent that transfer from being classified as a "sale"[7] of personal information. And if no sale has occurred, that transfer of personal information to the ad-tech vendor would not (taken alone) require the business to post a "do not sell my personal information" link[8] and would not be subject to a consumer's opt-out choice.[9]

However, the use of service provider contracts also has several drawbacks, which include:

- Significantly curtailing the activities an ad-tech vendor can undertake for a business when acting as a service provider due to the tight restrictions the CCPA places on service providers' processing of personal information.
- Unhealthy market dynamics that may damage both the ability of publishers to monetize ad inventory and the ability of advertisers to run transparent and efficient digital ad campaigns due to further concentrating ad spend in walled gardens.
- Increased compliance risks presented by complex, highly restrictive, and sometimes conflicting service provider provisions.

These drawbacks are discussed in greater detail below in Section II, followed by an explanation of promising alternatives to service provider contracts in Section III.

---

[1] CAL. CIV. CODE §§ 1798.100 *et seq.*

[2] *See, e.g., CCPA Amendment Tracker,* INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, https://iapp.org/resources/article/ccpa-amendment-tracker/ (Last updated Sept. 8, 2020).

[3] *See, e.g., CCPA Regulations*, CAL. DEP'T OF JUSTICE, OFFICE OF THE ATTORNEY GEN. (compiling the proposed CCPA regulations, modifications thereto, and associated materials), https://oag.ca.gov/privacy/ccpa/regs.

[4] *See* Press Release, Attorney General Xavier Becerra, Attorney General Becerra Issues Statement on Day One of CCPA Enforcement: Know Your Responsibilities (July 1, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-statement-day-one-ccpa-enforcement-know-your; Press Release, Attorney General Xavier Becerra, Attorney General Becerra Announces Approval of Final Regulations Under the California Consumer Privacy Act (Aug. 14, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-final-regulations-under-california.

[5] CAL. CIV. CODE § 1798.140(v) (defining "service provider").

[6] *Id.* § 1798.140(o) (defining "personal information").

[7] *Id.* § 1798.140(t) (defining "sale").

[8] *See id.* § 1798.135(a)(1).

[9] *See id.* § 1798.120(a) (setting forth a consumer's right to opt out of the sale of personal information).

II. Drawbacks to "service provider" relationships with ad-tech vendors

A. Service provider relationships may limit the services ad-tech companies can provide and affect business results for all parties

Businesses generally have good motivations for seeking new service provider contracts with their ad-tech partners. For example, they may be seeking to minimize their CCPA compliance risks, or assert greater control over how data about their customers is used for reasons that go beyond CCPA compliance. However, service provider relationships as defined by the CCPA are often a poor vehicle to achieve those goals. More than merely technical contract updates, service provider relationships may alter what ad-tech vendors can and cannot do for their clients, potentially limiting critical functions that are at the core of the digital advertising ecosystem. That is because service provider restrictions may in some cases be inconsistent with how data are actually used to provide services, especially when the data ad-tech companies collect from multiple clients are used for the benefit of all of those clients, not just one in isolation.[10]

With those restrictions in mind, ad-tech vendors engaged in interest-based advertising[11] and other related activities may not be able to provide those services to clients who insist that their ad-tech partners operate strictly as service providers. While each ad-tech vendor may use different technologies and different data flows to serve its clients, several prominent ad-tech companies have indicated that they will act as service providers for their clients only while substantially limiting the kinds of services they offer.[12]

---

[10] *See, e.g., id.* §§ 1798.140(v); 1798.140 (t)(2)(C) (prohibiting service providers from further collecting, selling, or using personal information obtained in the course of providing services except as necessary to perform the business purpose specified in the service provider contract). Indeed, the OAG has emphasized the importance of using personal information collected while acting as a service provider solely for the benefit of the business that provided it, stating that certain provisions in the regulations are "necessary to ensure that a service provider's internal use of personal information does not functionally operate to make personal information available to multiple businesses." The OAG has also warned that if a service provider were to make available to multiple businesses personal information obtained in the course of providing services to one business, doing so "would constitute a sale. . . and effectively usurp the consumer' right to prevent the sale of their personal information" because it is done while purportedly acting as a service provider. *See* CAL. DEP'T OF JUSTICE, OFFICE OF THE ATTORNEY GEN., FINAL STATEMENT OF REASONS, UPDATE OF INITIAL STATEMENT OF REASONS 34 (2020) [hereinafter FSOR], https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor.pdf.

[11] *See*, *e.g.,* NETWORK ADVERTISING INITIATIVE, 2020 NAI CODE OF CONDUCT § I.G (2020) (defining Interest-based Advertising as "the collection of data across web domains owned or operated by different entities, or the use of such data, for the purpose of tailoring advertising based on preferences or interests known or inferred from the data collected."), https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf.

[12] *See, e.g., Helping advertisers, publishers, and partners comply with the California Consumer Privacy Act (CCPA),* GOOGLE: BUSINESSES AND DATA (last visited Aug. 27, 2020) (Indicating that Google will act as a service provider subject to the terms of its CCPA service provider addendum while restricted data processing is enabled. While restricted data processing is enabled, Google has indicated it will not "create or update profiles for ads personalization or use existing profiles to serve personalized ads relating to data to which restricted data processing applies" or "[add] to or [update] remarketing lists using data to which restricted data processing applies" for certain products. Those restrictions would likely affect both publishers' ability to monetize inventory and advertisers' ability to reach their target audiences.), https://privacy.google.com/businesses/rdp/. *See also Helping Businesses Comply With the California Consumer Privacy Act (CCPA)*, FACEBOOK FOR BUSINESS (June 23, 2020) (indicating that businesses may "direct Facebook to process information about people in California as the business's Service Provider" while a

An ad-tech vendor's inability to provide certain services while acting as service provider is likely to degrade business results for all parties, resulting in reduced ability for advertisers to reach audiences and measure interest-based advertising campaigns (and thereby minimize advertising waste); decreased revenue for publishers; and fewer and less robust services that ad-tech vendors would otherwise be able to offer their partners. Further, overly-restrictive service provider terms may even substantially limit the ability of ad-tech vendors to assist advertisers in using their own customer data to target and measure ad campaigns. Those limitations would not necessarily apply only to programmatic campaigns – inappropriately restrictive data processing terms could impede an advertiser's ability to use ad–tech vendors to fulfill and measure campaigns that have been bought and sold directly, or that only make use of a publisher or advertiser's first-party audience data.

In sum, the way service provider agreements seek to limit the processing of personal information by vendors may prevent many vendors from engaging in the data processing necessary to provide their services, or limit their operations to the point where the service is rendered ineffective.

B. Restrictive service provider terms can have anti-competitive results.

The "service provider" limitations created by the CCPA are stringent by themselves, but some publishers and advertisers are seeking contract terms with their ad-tech vendors that go beyond the CCPA's requirements for "service provider" relationships – for example, they may seek to prohibit *any* data use by the vendor except for the sole purpose of providing services, including a prohibition on internal uses by the vendor to improve or enhance its own platform or services.[13] However, many of the valuable services ad-tech companies provide rely on processing data obtained through all of their clients collectively, whether in device-identifiable, aggregated, or anonymized form (e.g., for frequency and recency capping, measurement, analytics and optimization). Ad-tech vendors use that collective information to enhance the quality of the services they can provide to each of their clients individually. As such, overly-restrictive service provider terms may hamper the ability of third-party ad–tech vendors to innovate, putting them at a competitive disadvantage while benefiting larger first-party incumbents. This further shifts the advantage to first-party platforms that can use their own data to improve and enhance their systems. This dynamic allows walled gardens to continue to enhance their products and services, while disadvantaging third-party ad-tech companies and the businesses they serve.

As a result, and over time, publishers may see their ability to monetize ad inventory suffer if they prevent their vendors from using data to improve their own platforms and services. This free-rider problem will harm the digital advertising ecosystem as a whole by hampering the ability of third-party ad-tech companies to compete with large, first-party platforms. Advertisers are presented with the same kind of problem. If advertisers continue to press for unnecessarily tight restrictions on the use of data by their vendors to avoid an artificially broad notion of "selling" personal information, those advertisers are likely to see reduced value in the measurement and conversion services they rely on, and an overall reduction in the value of interest-based advertising for reaching their audiences. Over time,

---

Limited Data Use feature is enabled, and noting that "businesses may notice an impact to campaign performance and effectiveness, and retargeting and measurement capabilities will be limited" while Limited Data Use is enabled.), https://www.facebook.com/business/news/helping-businesses-comply-with-the-california-consumer-privacy-act-ccpa.

[13] *Cf.* CAL. CODE REGS. tit. 11, § 999.314(c)(3) (permitting service providers to use personal information obtained in the course of providing services to build or improve the quality of its own services under certain circumstances).

this may drive additional ad spend to large first-party platforms where advertisers may ultimately have to pay higher prices for the same quality impressions, and rely on those first parties to "grade their own homework" with respect to measurement, attribution, and other metrics.

C. Over-reliance on service provider agreements presents compliance risks

While some businesses are seeking service provider agreements with vendors primarily to provide a safe and CCPA-compliant way to meet their marketing and/or revenue goals using tailored advertising, service provider agreements may lead to their own compliance risks.

It is still unclear under the law and implementing regulations, and therefore unknown, how the OAG will interpret the service provider provisions in the CCPA as they apply to specific digital advertising use cases. As such, additional compliance risk accrues to publishers and advertisers if the contracts they use to designate ad-tech vendors as service providers are determined by the OAG to be inconsistent with the requirements of the law. In that case, depending on the facts and circumstances, there is a risk that the publisher or advertiser will be considered to have sold personal information to a third-party ad-tech vendor without posting a required "Do Not Sell My Personal Information" link,[14] or in contravention of a consumer's request to opt out of sales of personal information.[15] This has the further potential effect of mingling personal information subject to service provider terms with unrestricted data in the ad-tech ecosystem, although downstream vendors may lack transparency into such data commingling.

In addition to risks presented by the possibility of inadvertent sales of personal information, businesses relying on service providers must also deal with the added complexity of responding to consumer requests for access to or deletion of personal information in concert with their service providers. For example, the regulations state that when a service provider receives such a request in its capacity as a service provider, it shall either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.[16] Businesses that use service providers have to decide which approach to take and how to implement it. Further, if a consumer directs a request to delete personal information to a business, the business must comply with a valid request *and* direct any service providers to delete the consumer's personal information from their records.[17] Effectively communicating those deletion requests to multiple ad-tech vendors as required by the law – and being able to demonstrate compliance with the requirement to the OAG if necessary – may prove challenging.

Service providers are not solely responsible for managing these compliance risks. Depending on the circumstances, both a service provider and the business that engaged the service provider may be liable for uses of personal information that do not satisfy the CCPA's requirements. While a service provider is liable for its own failure to meet those requirements,[18] the business that has engaged the service provider is also liable for violations if the business actually knows, or has reason to believe, that the service provider will commit such a violation.[19] While we may not know for certain what specific activities a service provider may engage in unless the OAG begins taking enforcement actions on that

---

[14] *See* CAL. CIV. CODE § 1798.135(a)(1) (requiring businesses that sell a consumer's personal information to post a "Do Not Sell My Personal Information" link).
[15] *Id.* § 1798.120(d).
[16] CAL. CODE REGS. tit. 11, § 999.314(e).
[17] CAL. CIV. CODE § 1798.105(c).
[18] *See* FSOR, *supra* note 10, at 33.
[19] CAL. CIV. CODE § 1798.145(j).

issue, this is an area to watch closely and acknowledge the attendant compliance risk.[20] Publishers and advertisers should also bear in mind that the costs of any violations can add up quickly on a "per violation" basis in a programmatic environment – $2,500 for each violation or seven thousand five hundred dollars $7,500 for each intentional violation.[21]

III. Alternatives to service provider relationships

Publishers and advertisers should be actively exploring alternatives to service provider arrangements with their ad-tech vendors to avoid the negative side-effects and potential compliance risks discussed above. While service providers may have a limited role to play in facilitating digital advertising transactions, over-reliance on them unnecessarily diminishes an important value that many ad-tech companies bring to digital advertising – their ability to use information collected from across sites and clients to optimize bidding and increase monetization for all of them. This is a rising tide that lifts all boats.

Possible alternatives to service provider agreements include classifying ad-tech companies as either the business that collects personal information on the publisher page in certain circumstances,[22] or as "third parties"[23] to whom personal information is transferred or sold. While taking these alternative routes may lead some businesses to conclude that posting a "Do Not Sell My Personal Information" link is necessary where it otherwise would not be, those businesses will also be better positioned to realize important benefits and reduced compliance risk by doing so. These potential benefits include the following:

- Ad-tech companies can continue to offer a full range of products and services to their clients when acting as third parties,[24] without the compliance risks attending service provider arrangements (subject to a consumer's right to opt out of those activities that constitute "sales" of personal information). This allows for enhanced monetization for publishers and better reach and metrics for advertisers compared to service provider arrangements.
- The ability to use existing tools in the marketplace that allow publishers and advertisers to effectuate a consumer's request to opt out of "sales" to third parties that do not rely on complex contractual relationships. This includes the IAB's U.S. Privacy string[25] and the DAA's CCPA Opt-Out Tools for web and mobile.[26]
- When publishers or advertisers are working with ad-tech vendors registered as data brokers in California, there is a significantly lower risk that any potential downstream sales of personal

[20] *See, e.g.,* Letter from Center for Digital Democracy *et al.* to the Interactive Advertising Bureau (Nov. 5, 2019) (expressing skepticism about the ability of a standard service provider agreement developed by the IAB to satisfy the CCPA's requirements), https://advocacy.consumerreports.org/wp-content/uploads/2019/11/Consumer-and-Privacy-Group-Comment-on-IAB-CCPA-Framework.pdf.
[21] CAL. CIV. CODE § 1798.155(b).
[22] For example, some observers believe an ad-tech company that sets its own cookie on a consumer's web browser is accurately described as the business collecting information directly from the consumer, in which case it would not be a third party. *See id.* § 1798.140(w).
[23] *See id.* (defining "third party").
[24] Or, if applicable, businesses that collect personal information. *See id.*
[25] *See* IAB TECH LAB, IAB CCPA COMPLIANCE FRAMEWORK FOR PUBLISHERS & TECHNOLOGY COMPANIES, https://iabtechlab.com/standards/ccpa.
[26] *See* DIGITAL ADVERTISING ALLIANCE, OPT OUT TOOLS, https://www.privacyrights.info.

information collected through a publisher or advertiser site would fail to meet the CCPA's notice and choice requirements.[27]

- Advertisers and publishers are not required to coordinate with third parties in connection with verified consumer requests to access or delete personal information. This removes a significant complication attending service provider relationships because a business is required to direct its service providers to process deletion requests.[28] Because ad-tech companies generally do not have a direct one-to-one relationship with the consumer and often rely on aggregate or pseudonymous data, it is difficult to delete information in response to an single business's request without getting more information about the consumer. Even after receiving such information, deletion may not be possible because of the pseudonymized or anonymized/aggregated nature of the data.
- Businesses seeking to respond adequately to a consumer's request to know[29] may be required to gather information about that consumer from its service providers, which may be difficult in a programmatic environment. No corresponding difficulty arises for third party relationships because there is no requirement for third parties to participate in requests to know or delete made to a different business.
- Many of the largest and most reputable publishers and advertisers have already elected to post a "Do Not Sell My Personal Information" link to enhance transparency and choice for California consumers, which should mitigate any perceived reputational risks associated with posting a link. See **Appendix A** for a list of such companies. Businesses that post "do not sell" links are also in a position to avoid certain compliance risks associated with over-reliance on service provider relationships discussed herein. Note, however, the fact that these businesses have determined to post "do not sell" links does not necessarily imply a conclusion on their part that using third-party ad-tech vendors involves "selling" personal information.

[27] According to the implementing regulations, companies that register as data brokers do not have to provide a separate notice at collection to consumers. *See* CAL. CODE REGS. tit. 11, § 999.305(e). Further, there is strong evidence that the requirements under section 1798.115(d) of the CCPA for downstream sales are also satisfied by registration as a data broker. *See* FSOR, *supra* note 10, at 11.

[28] *See* CAL. CIV. CODE § 1798.105(c).

[29] *See* CAL. CODE REGS. tit. 11, § 999.313.

Appendix A:

Top 10 Desktop Internet Display Advertising Spenders (2019) (source: Ad Age Leading National Advertisers 2019 Report, https://adage.com/article/datacenter/ad-age-leading-national-advertisers-2019-index/2178026) (businesses that have posted a DNS link are in **bold)**:

1. Amazon (www.amazon.com)
2. **Comcast Corp.(https://corporate.comcast.com/)**
3. **Verizon Communications (https://www.verizon.com/about)**
4. **Expedia Group (www.expedia.com)**
5. Axel Springer (https://www.axelspringer.com/en/)
6. **Dish Network Corp. (www.dish.com)**
7. U.S. Government
8. **Fiat Chrysler Automobiles (e.g. www.chrysler.com)**
9. Progressive Corp. (www.progressive.com)
10. Bed Bath & Beyond (www.bedbathandbeyond.com)

Top 10 Publishers by page view (2017) (source: https://www.statista.com/statistics/591483/media-publishers-us-online-traffic/)
(businesses that have posted a DNS link are in **bold)**

1. Microsoft (msn.com)
2. **Drudge Report (drudgereport.com)**
3. Google (news.google.com)
4. **ESPN (https://www.espn.com/)**
5. **CNN (cnn.com)**
6. **yahoo! (e.g. finance.yahoo.com)**
7. **Fox News (https://www.foxnews.com/)**
8. **New York Times (www.nytimes.com)**
9. **Washington Post (www.washingtonpost.com)**
10. **Buzzfeed (www.buzzfeed.com)**