Cybersecurity Law Report
An Acuris company

cslawreport.com

February 19, 2020

ONLINE ADVERTISING

Consciously Coupling: Tackling the Juxtaposition Between Adtech and Privacy

By Sarah Bruno and Casey Perrino, *Reed Smith*

The onslaught of privacy regulations has impacted every industry and, while it seems that no industry can be flat footed – from auto manufacturers to ecommerce platforms – one in particular has had to remain especially nimble: the advertising technology (Adtech) industry. In this article, we discuss the growth of Adtech and how it falls into privacy laws' crosshairs, review relevant definitions under the CCPA and provide advice on how the industry can comply with the patchwork of sometimes allusive definitions, including by turning to industry tools and knowing their data.

See also "Key Compliance Considerations for Fund Managers Using Alternative Data" (Jan. 15, 2020).

Growth of Adtech

In the last few years, the term "Adtech" has grown from a well-known concept in the advertising and ad agency realm to a term that is now populating the discussion boards of privacy practitioners. There are two reasons for this: (1) data, and what can be learned from it, which is the currency of the Adtech industry; and (2) new privacy regulations that have stretched the definition of "personal information" to potentially encompass the data collected and exchanged via ad networks.

It Starts With Data

With data serving as the currency exchanged via these networks, advertisers and agencies want to get the most out of their dollars by running effective advertising campaigns to reach their target audiences, optimizing these campaigns, measuring return on investment and gathering consumer insights. The data collected from consumers when advertisements are delivered can have a hand in determining these goals, as it may help a brand appreciate consumer patterns, understand the effectiveness of an advertisement, and "remind" consumers about a product or suggest an alternative to one that the consumer has been keeping an eye on. Publishers – or the websites on which the ads are placed – also want to understand what consumers are doing on their websites, and which ads are working. Publishers must ensure the ads on their platforms are generating more visitors and more impressions, but they also want to know what actions consumers are taking on their websites or apps, what content is effective and what content may need to be put on a virtual shelf because consumers are not paying attention to it. The data collected via cookies and pixels drives these decisions as well.

Adtech's Role as Facilitator

Adtech provides the tools and technologies that facilitate the collection, analysis and use of the data so that advertisers and publishers ensure their content, products and services are relevant and consumed. The data collected may include referring websites (*i.e.*, where the visitor came from), the visitor's overall journal on the website (*e.g.*, cursor movement), events (*e.g.*, scrolling, clicks, highlights, media views), search queries, session times, demographics, information about the visitor's device (*e.g.*, browser specifications), and interaction with advertising content. Understanding what data is collected and why it is collected is now a very important part of the analysis, as this is what drives the privacy side of the analysis.

CCPA Privacy Concerns and Opportunities

As technology and data become more prominent, privacy has become an increasing concern of consumers, companies and lawmakers. Whether data is deemed PI weighs heavily on how to address these concerns. Until recently, the term "personal information" in the United States had been limited to information that most would consider as personal, starting with name and address and moving all the way up the chain of sensitivity to medical or financial data. California changed the game in 2018.

The CCPA imposes new obligations on covered businesses and grants new privacy rights to California consumers, such as the right to know what PI a business holds on that consumer, the right to request the deletion of certain PI and the right to opt out of the sale of PI.

See also CSLR's two-part series on CCPA priorities: "Turning Legislation Prep Into a Program Shift" (Jun. 5, 2019); "Tackling Data Subject Rights Requests and Vendors" (Jun. 12, 2019).

"Personal Information" and "Selling" Under the CCPA

Under the CCPA, PI means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer or household. Because of how expansive this definition is, much of the data collected by Adtech could be considered PI.

For this reason, the announcement of the CCPA shook the Adtech industry. If information that could "reasonably be linked" to a consumer is PI, the concern was that much of the information collected online from California consumers is PI and therefore subject to the potentially onerous requirements of CCPA.[1]

One such requirement is that a company provide consumers with a right to opt out of the "sale" of their PI. A "sale" is defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration." In practice, this means that depending on the context, the exchange of PI collected by pixels or metatags via advertising exchanges or other programmatic advertising may constitute a "sale" under the CCPA, which would trigger the requirement for an opt-out.

If a "sale" occurs, the party in direct proximity with the consumer – often the publisher – must provide California consumers with an ability to opt out of that sale via a "Do Not Sell My Personal Information" or "Do Not Sell My Info" link or button on that party's website homepage or in that party's mobile application settings menu. Once a consumer clicks on the link or button, that consumer must be taken out of all exchanges of PI that are considered a "sale" and the opt-out must also be communicated to any parties to which the PI has been "sold." Practically speaking, this would be a very difficult requirement for any company to implement, but especially a company that is "downstream" from the data collection and which may not be in a position to fulfill an opt-out request as a result of its position in the stream of collection.

See "How to Approach CCPA's Under-16 Opt-In Consent" (Feb. 12, 2020).

Similar Legislation

Bills and laws similar to the CCPA have been introduced in the United States.[2] Nevada has a law currently in effect, and a number of state privacy bills have been introduced, with similar provisions that require companies to allow consumers to opt out of the sale of their PI. Nevada's law refers to "covered information" which includes any information "concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable." But Nevada's definition of sale is limited to "the exchange of covered information for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons."[3]

The proposed Washington Privacy Act, if passed, would be the most comprehensive privacy law in the country, going further even than the CCPA and E.U. law. Thus, the issue of control over the sale of PI shows no signs of abating any time soon, but fortunately, the advertising industry has been hard at work developing solutions of different shapes and sizes.

See "Implications of Nevada's New Privacy Law" (Jul. 10, 2019).

Two Workarounds

There is some relief provided by the CCPA. The CCPA excludes from the opt-out requirement the exchange of data between a business and its "service providers" – that is, entities that processes PI on behalf of the business. In order to fall within the definition of "service provider" a company must establish that there is a written agreement that limits the service provider's use of the PI to the provision of services for that business – from the definition of sale. If the PI flows to a "service provider," it is not considered a "sale" and is not beholden to the opt-out requirements.

Another potential avenue for relief is within the definition of PI. For one, the proposed regulations may limit the definition by excluding information that is not maintained in a manner that allows it to be linked to an identified consumer or household.[4] Second, the CCPA does not apply to information that is aggregated or de-identified. Aggregated information is information that relates to a group or category of consumers, from which individual consumer identities have been removed. De-identified data is information that cannot reasonably identify an individual, so long as the business has implemented safeguards to prohibit reidentification. For

some companies in the Adtech space, these two buckets of data provide additional avenues for avoiding the requirements of the CCPA.

See also "Updating Vendor Agreements to Comply With CCPA: Service-Provider Exemption and Corporate Approaches" (Nov. 6, 2019).

The Conscious Coupling: How Adtech Faces the Challenge

The Adtech industry has struggled with privacy regulations, including the CCPA, but it has taken the reins of the challenge. Some players have added language to their agreements to ensure they are considered service providers, while others are focused on the definition of PI and developing systems to ensure the data they receive or share falls outside of it. While the effectiveness of these solutions and whether they are compliant with the CCPA will likely be tested in the coming year, they give companies in the Adtech ecosystem a few attractive options for compliance with the requirement to allow consumers to opt out of the sale of their PI.

DAA Tool

The industry has developed technical solutions to assist companies with the steps needed for compliance with the more challenging requirements, such as the opt-out of sale of PI. For example, one of the options being used today includes the Digital Advertising Alliance's (DAA) CCPA tool, which enables consumers to click on an opt-out icon on publisher websites and mobile applications that notify all participating companies that the consumer has requested to be removed from the sale of PI. Companies that participate in the DAA's self-regulatory program and that receive the request must stop the sale of that consumer's PI. The benefit of the DAA tool is that it uses a clear and recognizable icon – similar to the one that many consumers will know from the YourAdChoices program – to indicate consumer choice.

IAB Compliance Framework

Another option comes from the Interactive Advertising Bureau (IAB), which has developed the "CCPA Compliance Framework for Publishers and Technology Companies." The framework consists of a Limited Service Provider Agreement, as well as technical specifications to facilitate CCPA compliance through ad exchanges. The framework aims to provide Adtech companies with assurances that participating publishers comply with the CCPA's notice and opt-out requirements, while at the same time providing publishers with assurances that technology companies will use PI only for "business purposes" permitted by the CCPA when consumers exercise their right to opt out.

A "business purpose" is limited to use of the PI for the business's, or that business's service provider's, operational or other notified purposes. The framework requires participating publishers to provide clear and conspicuous notice of consumers' rights under the CCPA and what will happen to their PI. Companies that sign on to the agreement commit to functioning as "service providers" when a request to opt out is received. This means that when a consumer opts out of the sale of their PI, a CCPA signal is sent to downstream technology companies notifying those companies to refrain from practices that are or may be considered "selling," and to switch to practices that would put them in the

"service provider" bucket. This means their use of the PI at issue will convert to only those uses necessary to provide their service to the business. The signal is made via a technical mechanism based upon specifications developed by the IAB Tech Lab.

Google Settings

Google has also thrown its hat in the ring by introducing settings that allow for "restricted data processing" to help publishers comply with the CCPA. These restricted settings allow a company to limit Google's use of that company's consumers' PI to only service-related functions, similar to the mechanism supported by the IAB. When these settings are activated, Google will only serve non-personalized advertisements. It also offers service-provider terms under the CCPA that aim to supplement Google's existing data protection terms. Google's tool offers a certain amount of flexibility. Some publishers will choose to activate this restricted setting for all of their programmatic traffic for California consumers. Others may choose to send a restricted data processing signal on a per-request basis when a consumer opts out.

Four Practical Compliance Tips

While companies will still need to keep an eye on inevitable further developments in this area, the following practical tips may aid them in the Adtech sphere in their compliance efforts:

1. Know your data. As a starting point, it is important to know the types of data at issue. This will help to classify the PI that may be collected and identify PI that you may not need to collect to for your purposes. This can be accomplished through a company-wide data audit or data mapping exercise. The process is usually overseen by legal or the privacy team and involves an analysis of all the data collected by an organization and a consideration of how a company acquired the data and where (or with whom) it was stored. The scope of the audit depends on the size and complexity of the business and the nature of the data that is collected. A company will need to evaluate all the potential locations for data and consider what individuals should be involved in the process, but typically the list of stakeholders includes individuals from HR, marketing, IT, legal and contracts/procurement.
2. Choose to aggregate or deidentify when possible. Once you have identified what PI you collect, it may be helpful to categorize the data to determine whether the information could still be useful for your business or commercial purposes in a de-identified form. For example, if your business maintains a data set that includes a user's first name and email address, as well as an advertising ID, media views and search queries, you may consider removing the name, email address and advertising ID from that data set. Certainly, if your business is able to utilize the remaining data – media views and search queries – even though it does not identify a particular consumer, deidentifying that data set may be an attractive option as it removes that data from the scope of additional privacy requirements.
3. Maintain your data as non-personal information. The revised CCPA regulations indicate that if data is maintained in a manner that does not allow it to be linked with an identifiable consumer or a household, then it is not considered PI. For example, imagine a scenario where Jane

Doe is browsing on Publisher X's website, which contains a cookie dropped by Company Z that collects (i) information about Jane's interactions with the advertisements on the website and (ii) her IP address. Company Z has no other information about Jane; it does not know her name, email address, age, gender or device ID. If Company Z stores the data it collects via the cookie separately from Publisher X's data, under the proposed revisions to the CCPA regulations, the data that Company Z collects may not be considered personally identifiable. However, if Publisher X combines the data it has collected about Jane – including her name, mailing address and purchase history – with the information it receives from Company Z's cookie, then the combined data (*i.e.*, Publisher X data + data from Company Z cookie) would be considered PI.

4. Consider whether you are a service provider or a business. By analyzing the ways in which you will use the PI you collect – for example if you are using the PI solely for the benefit of another company with which you work or if you are using the PI for your own commercial purposes – you can determine whether the requirements to respond to requests to opt out of the sale of PI apply to you.

Sarah Bruno is a partner in Reed Smith's San Francisco office. She is a trusted advisor to companies in the retail, technology, entertainment, gaming, automotive and association spaces, and counsels her clients on the privacy, advertising and marketing legal requirements for the development and launch of their platforms, products and services.

Casey Perrino is an associate in Reed Smith's San Francisco office whose practice focuses on data privacy and security counseling, which includes reviewing the evolving data privacy landscape to determine how new or amended laws may affect her clients' business practices and privacy programs.

---

[1] It is important to note that the California Attorney General's modified proposed regulations, which were released on February 7 and are open for public comment until February 25, provide some comfort by clarifying that whether information is personal information under the CCPA depends on whether the business maintains information in a way that makes it reasonably capable of identifying an individual. By way of an example relevant to the Adtech industry, IP addresses of website visitors are not personal information if the business does not link the IP address to any particular consumer, and could not reasonably link the IP address with a particular consumer. This may help some companies avoid falling within the CCPA's ambit.

[2] See, *e.g.*, Nev. Rev. Stat. § 603A.340; and Washington's SB 6281.

[3] Nev. Rev. Stat. § 603A.320 and 603A.333.

[4] California Consumer Privacy Act Modified Proposed Regulations § 999.302.