Data Privacy Monitor
Commentary on Data Privacy & Information Security Subjects

BakerHostetler

Ad and Publishing Industries Confront CCPA Challenges While Congress Considers Privacy

By **Alan L. Friel** on May 29, 2019
Posted in **CCPA**

The California Consumer Privacy Act (CCPA), effective Jan. 1, 2020, will require more privacy transparency and choice for consumers than they have ever had under U.S. law, but its approach to providing consumers with the right to opt out of a sale of their personal information threatens to disrupt the third-party digital advertising ecosystem. Most consumers are aware that adtech has evolved to enable tracking technologies to monitor online usage across time and sites in order to build interest profiles tied to pseudonymous identifiers and thereby permit advertisers to send ads tailored to likely interests. Consumers benefit from getting more relevant ads, which advertisers will pay more to place, which in turn generates more revenue for publishers, thereby fostering free, ad-supported content that also benefits consumers. Win-win, right? Not so fast, some say; tracking and targeting is intrusive, or at least creepy, and consumers should have a choice about who can learn what about them and use that information to advertise to them. In response to that consumer concern, the U.S. advertising industry developed a transparency and choice paradigm that relies on notices and opt-outs. (Learn more about that here and here.) In addition, users of online services can employ techniques such as using ad blockers and limiting cookies. Google recently announced that it will ban device fingerprinting for ad personalization, citing lack of user transparency and control, and will enable users to block third-party cookies, a typical adtech tool, while permitting first-party cookies, a typical publisher tool. However, the CCPA is poised to upset this approach to consumer choice through its “do-not-sell” right, which provides an opt-out choice for consumers age 16 and older, but requires opt-in for youth between 13 and 16, and parental consent for children under 13.

This is because the CCPA's broad definitions of "personal information" and "sell" threaten to include the passing along of adtech data tied to a particular device to enable third-party interest-based advertising (IBA) within the scope of the do-not-sell right. Unlike first-party advertising, where a publisher serves an ad based on its own data and potentially data supplied by the advertiser, third-party IBA exchanges data among a myriad of intermediaries in a complex digital ecosystem. As a result, even small publishers can sell ad inventory through this ecosystem that matches advertisers, publishers and online consumers in a fraction of a second to facilitate the sale and delivery of ads tailored to the perceived interests of the consumer. This helps publishers of all sizes compete for ad dollars with tech giants, such as the ubiquitous social media sites and search engines, and large publishers, which have their own treasure trove of consumer data they can use to tailor ads. CCPA does not disrupt that kind of first-party targeting because consumer information is not shared with third parties to enable the sale and delivery of a tailored ad. It is not an exaggeration to say that third-party IBA is what keeps a wide array of online content available to consumers for free. And consumers who object to IBA can opt out of it through the industry opt-outs that are linked to from ads and the website pages that display those ads.

The problem CCPA creates, however, is that the technology supporting that opt-out essentially sets a flag to tell the IBA ecosystem players not to serve an IBA ad. If you don't want that pair of shoes you were considering buying to follow you around in the form of online ads, then you should opt out. And the ad industry's self-regulatory rules, available here and here, prohibit certain forms of sensitive or intrusive IBA. CCPA's opt-out remedy, however, addresses the data sharing, not the data use. So upon the receipt of a CCPA do-not-sell request, a business will be obligated not to share or make personal information available "to another business or a third party for monetary or other valuable consideration." There are a number of sound theories for why that restriction should not restrict IBA data transfers, as the Network Advertising Initiative (NAI) explains in its comments and proposed draft regulations to the California attorney general (AG), who is tasked with promulgating regulations to implement CCPA. Adoption of the NAI's recommendations would bypass the effect the do-not-sell right would have if applied to IBA. A proposed bill to amend the CCPA's definition of sale to specifically carve out IBA data transfers, SB-753, was pulled by the author before advancing to necessary hearings and will not make it out of the Senate by the May 30 deadline for passing its house of origin, killing any chance of the bill passing this year. It was opposed by many privacy advocates, including Californians for Consumer Privacy (CCP, the group that initiated CCPA in the first place), who argued that a primary purpose of CCPA was to limit the sharing of consumer information for advertising beyond a limited silo of first-party advertising:

> **"Under CCPA, a business can use a "consumer's information to show advertising on its own website, or use an advertiser, acting as a service provider or contractor to show ads on the business' website as long as the information shared by the business about the targeted consumer is siloed between the business and the advertiser. … [However,] SB-753 proposes to amend the definition of "sell" in Civil Code Section 1798.140 in a manner that will break down th[is] silo effect. … As a result, even if a consumer opts out of the sale of their data, this proposal would allow an advertiser to combine,**

share and proliferate data throughout the advertising economy. The proposed language will essentially eliminate the silo effect that would occur pursuant to the CCPA, which allows for targeted advertising but prevents the proliferation of a consumer's data throughout the economy."

The CCP's interpretation of the CCPA's intent, or at least the ballot initiative they drafted that is the precursor of CCPA, would be inconsistent with the NAI's interpretation and recommendations. We will have to wait until the first set of proposed rulemaking is issued in September to find out whether the AG agrees with the CCP or the NAI. In the meantime, businesses are struggling with how they can practically effectuate a do-not-sell request to IBA, and which parties, between the publisher, advertiser and various intermediaries, are even responsible for doing so, as well as whether there is a statutory exception on which they can rely for not treating the data flow as a sale.

As we have written before, the online advertising industry has been struggling to address compliance challenges with the EU's relatively new General Data Protection Regulation (GDPR), which takes a different approach to choice than the CCPA does but presents similar choice management challenges. On the eve of the effective date of the GDPR, the Internet Advertising Bureau (IAB) Europe and the IAB Tech Lab launched an open-source Transparency and Consent Framework (TCF), a version 2.0 of which is about to roll out and is expected to have greater industry adoption, including by Google. One solution for CCPA may be to modify the TCF 2.0 to address CCPA application. However, the CCPA's approach of opting out on a business-specific basis, as opposed to using consent or legitimate purpose for processing-specific activities, would require a substantial revision of how the TCF is designed and implemented. Other technology-based solutions are under consideration by ad industry groups and compliance solutions providers. No CCPA consent management technology that would address IBA has yet to emerge, and we are only about six months out from the CCPA's effective date. Come September, if the California AG's proposed regulations do not provide assistance, there will be a need to rapidly reach industry consensus on how to address the problem.

Might help come from inside the Beltway? A coalition of ad industry trade associations known as Privacy for America is aiming to facilitate just such a fix. Specifically, it is working with the committees in the Senate and the House that are drafting a potential federal consumer privacy bill. The bill would develop a paradigm based on preventing harm and prohibiting certain data practices that are overly intrusive or have a potential to cause harm to consumers. Further, it would specifically not limit transfers of data for advertising purposes, including tracking and targeting, as long as sensitive data is not used and the use does not include making determinations on eligibility (e.g., for credit, housing or employment). But, opponents of IBA seem to have found an ally in the junior senator from Missouri, Republican Joshua Hawley. Introduced on May 21, Hawley's S. 1578 would require the Federal Trade Commission (FTC) to create and make available a "do-not-track" (DNT) signal that consumers can associate with their devices, which requires online services to look for the signal and, when indicated, not collect, use or share data beyond what is necessary to operate the service, and specifically not for IBA. It would further require that third-party operators, including

advertisers and adtech companies, not collect any data other than for the purpose of analyzing how or whether the user engaged with the operator's program, and then only in a de-identified manner and without creating or contributing to a user profile. The proposed law would prohibit publishers from denying service to users who enable a DNT signal or providing them with a different level of service. That prohibition would thereby ban publishers from charging a subscription fee for IBA-free access to make up for lost ad revenue (IBA commands higher prices than contextual or run-of-site ads), something that CCPA does not prohibit. The FTC, and state AGs, would be able to enforce the law, and it gives the FTC authority to seek civil penalties of $50 per affected user for negligent violations, and $1,000 per user and a minimum fine of $100,000 for reckless or willful violations. There is no private right of action proposed, and the bill does not preempt CCPA or other state law. This may be an attempt to influence the federal privacy legislation being drafted by congressional leadership in both chambers.

Finally, in the absence of federal preemption of state law, a patchwork of CCPA-inspired laws appears to be coming down the pike. Although legislation died in Washington and Texas, consumer privacy laws are advancing in Illinois, New Jersey and Nevada, and legislation has been introduced in Arizona, Hawaii, Maryland, Massachusetts (which has a private right of action), Missouri, New Mexico, New York, North Dakota, Oregon, Rhode Island and Virginia.

We will continue to track and report on refinements to CCPA; other legislation that may affect digital advertising, publishing and commerce; and the progress of industry in overcoming compliance challenges. For more information, contact the author.