Cybersecurity Law Report cslawreport.com

Apr. 17, 2024

Online Advertising

Tracking Technologies: Compliance Challenges and Solutions

By Michael Hahn, *IAB - Interactive Advertising Bureau*; Leslie Shanklin, *Proskauer*; Julie Rubash, *Sourcepoint*

The ecosystem and dynamic state of digital technologies, and the legal regimes around them, present companies with complexities that require thoughtful compliance and risk-mitigation strategies. This final installment of a four-part article series examines some of those compliance challenges and solutions specific to the digital advertising industry, as well as broader tracking use litigation risks and mitigation steps.

Part one kicked off this article series with a comprehensive review of the legal landscape around digital tracking. Part two took a deep dive into the technical workings and types of digital data collection tools. Part three provided a roadmap for organizations starting out – or working toward – crafting a comprehensive, cross-functional program for managing digital trackers.

See "Benchmarking the Impact of State Privacy Laws on Digital Advertising" (Oct. 11, 2023).

Ad Industry Challenges and Solutions

The complexity of data flows in the digital advertising industry, particularly with respect to programmatic advertising, requires a robust cross-functional approach to privacy compliance. That involves not only the types of data mapping, scans and other activities that happen within the four walls of companies and have been discussed in prior installments of this series, but also leveraging industry solutions to effectuate compliance.

Compliance Hurdles in a Complex Ecosystem

The OpenRTB technical specification, which undergirds programmatic advertising, created efficiency in the digital ad supply chain that greatly benefited advertisers, but also created numerous interconnectivity points involving disclosures of personal information. As a practical matter, to deliver and measure a single programmatic ad, there can be dozens of "sales" of personal information,

such as when supply-side platforms, ad exchanges or mediation platforms send out bid requests containing personal information in relation to a particular consumer (or their associated device), when measurement companies and other vendors include pixels in the ad impression, and more.

The complexity of the digital advertising ecosystem with respect to data exchanges, whether in the bidstream or facilitated by digital trackers, creates material compliance challenges for organizations. The obligations imposed by the California Privacy Rights Act (CPRA) amendments to the CCPA highlight these compliance challenges. Before this amendment, the CCPA required "businesses" to enter into contracts with their "service providers" containing certain privacy-protective provisions. While not underestimating the challenges of the contracting process, companies at least knew (or should have known) who their service providers were.

The CPRA amendment, however, greatly expanded the contractual requirements such that all "sales" of personal information to "third parties" must also be supported by contracts with prescriptive privacy provisions. While this requirement undoubtedly serves a very important privacy value, compliance can be challenging for certain "sales" that take place in the digital ad supply chain because, in at least some cases, entities disclosing and receiving personal information between each other do not have a formal business relationship governed by a commercial agreement.

For example, when an ad renders on a publisher's page, the publisher's ad server typically must disclose the consumer's IP address to the advertiser's ad server to retrieve the ad. No money is exchanged by the ad servers, and, as such, historically these ad servers have not entered into contracts with each other. Indeed, the publisher typically does not know which advertiser will win a particular bid to serve the ad or which advertiser's ad server will be used. Another example occurs when an ad renders on the publisher's digital property, and pixels or tags from advertiser-engaged vendors fire from within the ad impression itself. In permitting this to happen on its digital property, the publisher "makes available" personal information, such as IP address or other identifiers, to those vendors but the publisher typically does not have an agreement with those vendors or the underlying advertiser that has engaged those vendors as the advertiser's service provider. And again, the publisher often does not know which vendors will show up in the impression itself.

See "Lessons From California's First CCPA Enforcement Action" (Sep. 28, 2022); and "Lessons From California's DoorDash Enforcement Action" (Mar. 6, 2024).

IAB Solutions

Such compliance challenges in the digital advertising context, including the numerous "sales" occurring at different points in the digital ad supply chain, necessitate that the industry come together to create compliance solutions that publishers, advertisers and ad tech vendors would not be able to easily solve in individualized campaign transactions. Recognizing these challenges, the Interactive Advertising Bureau (IAB) has provided leadership in bringing industry stakeholders together and formulating proposed legal and technical solutions that complement each individual company's efforts to achieve compliance.

In the U.S., IAB Privacy's Multi-State Privacy Agreement (MSPA) provides a solution for the aforementioned gaps in contractual privity. The MSPA is a contract with privacy terms that "spring into place" among its network of over 1,200 signatories throughout the digital ad distribution chain. In other words, when a publisher's ad server "sells" personal information to an advertiser's "ad server" in the context of an MSPA transaction, and everyone is an MSPA signatory, the MSPA's contractual terms follow the data and endeavor to create the contractual privity between the participants that the law now requires.

More broadly, the MSPA creates a common set of privacy terms and principles throughout the distribution chain that seek to raise the bar for privacy and, in doing so, serve as a transparent tool to help companies achieve compliance with the ever-growing number of U.S. state privacy laws. For example, state privacy laws and implementing regulations increasingly require due diligence of counterparties with respect to data practices. The MSPA creates a compliance paradigm in which publishers and advertisers know the specific privacy terms that attach to personal information as it traverses the digital ad supply chain. Moreover, the MSPA avoids a party having to face a counterparty that has creative or myopic views of the how the privacy laws apply and seeks to link those views to privacy provisions that travel down the distribution chain. The MSPA sets a common set of compliant privacy terms for all market participants to point to.

The MSPA also creates a multi-state compliance framework that provides publishers and advertisers with an option to employ a national approach that leverages a highest common denominator across the state privacy laws and transmits privacy choices through the digital ad supply chain using the IAB Tech Lab's Global Privacy Platform signaling specification.

The complexity of the digital ad supply chain similarly necessitates an industry solution to comply with the ePrivacy Directive and the GDPR. IAB Europe's Transparency & Consent Framework (TCF) stitches together publishers, consent management platforms and adtech companies in a common framework to achieve compliance with the GDPR and ePrivacy Directive's applicable transparency and choice requirements. As the landscape has evolved in Europe, regulators are increasingly making clear that consent is required for behavioral advertising and may be required for activities such as measurement of digital ads. Given the unique role that publishers have in managing relationships with consumers, the TCF standardizes the means for obtaining consent from consumers for those publishers and downstream companies. Like the MSPA, the TCF relies on an IAB Tech Lab technical specification to transmit user privacy choices to companies participating in digital ad transactions.

Finally, the IAB Tech Lab is completing work on a deletion specification to solve for state privacy and GDPR deletion requirements. The comment period closes April 22, 2024. Again, the CPRA's amendment to the CCPA highlights the challenges of operationalizing certain requirements in the digital ad supply chain. Before this amendment, the CCPA required businesses to pass deletion requests to their service providers to act upon. The CPRA significantly expanded the scope of the deletion obligation, causing businesses to pass deletion requests to all third parties to whom the business "sells" personal information. That includes not only "sales" of personal information to other parties in the bidstream, but also "sales" of personal information that is transmitted by publishers or

advertisers through tracking technology. Given that a single ad can have dozens of "sales" associated with it, practical questions arise about how companies can achieve compliance. The IAB Tech Lab is addressing this fundamental challenge with its anticipated deletion specification, which will provide a standardized and interoperable framework to pass deletion signals to third parties and service providers.

For organizations involved in any aspect of the digital advertising ecosystem, particularly those engaged in or supporting programmatic advertising, industry solutions, such as those created by IAB, should be evaluated as a potentially important component to the company's privacy compliance program.

See "IAB Unveils Multistate Contract to Satisfy 2023 Laws' Curbs on Targeted Ads" (Feb. 22, 2023).

Tracker Litigation Risk and Mitigation

Even organizations that implement a gold-standard tracker governance program and utilize both state-of-the-art technology tools and evolving industry self-regulatory solutions face significant risk of privacy class action litigation in the U.S. related to tracking technologies.

See "Google's Wiretap Cases Highlight Evolving Privacy Transparency Standards" (Jan. 24, 2024).

VPPA and CIPA Claims

In addition to the most recent wave of Video Privacy Protection Act (VPPA) cases that have focused on social media pixels used in connection with website video content, the plaintiffs' bar is continuing to test case theories under the California Invasion of Privacy Act (CIPA). Not deterred despite many case dismissals under wiretap provisions of this law, a new flavor of these cases has taken hold in 2024 based on arcane provisions of CIPA that restrict use of "pen register" or "trap and trace" devices without a court order. Both class action and individual lawsuits have been filed, in addition to scores of claim letters being issued, asserting the credulity-stretching theory that website tracking technologies, even those used just for basic site analytics, violate these provisions that traditionally have been limited to physical devices (typically used by law enforcement) that record numbers dialed from a specific telephone line or the originating numbers of calls placed to the line.

See Cybersecurity Law Report's two-part series on website-tracking lawsuits: "A Guide to New Video Privacy Decisions Starring PBS and People.com" (Mar. 29, 2023), and "Takeaways From New Dismissals of Wiretap Claims" (Apr. 5, 2023).

Steps to Avoid Risk

As courts are put in the unenviable position of trying to make sense of the latest CIPA claim theory, organizations should consider taking the following steps to try to avoid being on the receiving end

of a complaint or claim letter.

- *Privacy Disclosures*: First and foremost, make sure your website privacy disclosures are accurate, robust and presented in a manner that does more than just tick the box of bare-minimum compliance. They should provide your company with the strongest protections against CIPA claims.
- *Cookie Banners*: Consider implementing a cookie banner on your website that is tailored for the unique risks posed by CIPA litigation. Banners should inform website visitors of the collection or recording of information through the use of tracking technologies and incorporate a form of consent – either implied or express, depending on the level of risk tolerance.
- *Suppressing Riskier Trackers*: If a cookie banner is used, consider configuring it to suppress riskier trackers until consent is provided, at least for California visitors. Riskier trackers may be ones that transmit the contents of communications, infer sensitive data or involve sharing data with third parties that have the right to use collected data for their own purposes.
- *Unnecessary Trackers*: As noted in part three of this series, engage in regular review of trackers incorporated into websites and apps, and remove trackers that are no longer providing material business benefit.

See "After Death of the Cookie, New Advertising Strategies Raise Compliance Questions" (Sep. 2, 2020).

Future-Proofing

As part of an overall digital tracking program, when implementing the practicalities above with the governance guidance set forth in part three, it is critical to consider ways to ensure the program is sufficiently nimble and scalable to adapt to both the organization's evolution and the dynamic state of digital technologies and legal regimes surrounding them.

Professionals with ownership over the program should keep pace with the growing risks and complexities around tracking technologies, as it is likely that organizations in the digital sphere will be facing ever-increasing risk and compliance requirements in the years to come. They should ensure that the company's overarching business and technology strategic processes include mechanisms to flag any changes to digital products, advertising methods and tech infrastructure that may impact tracker tech risk posture, compliance approaches or both. Business, technical and revenue teams also should be updated on legal and regulatory changes on the horizon that may impact compliance implementation and strategic planning.

Michael Hahn is executive vice president and GC at IAB and IAB Tech Lab. He has responsibility for all legal matters, including the direction of legal strategy, privacy compliance, antitrust compliance, intellectual property rights issues and general corporate matters. Hahn also serves as an advocate for the digital advertising industry on common legal issues affecting member companies.

Leslie Shanklin is head of Proskauer's global privacy & cybersecurity group, a partner in its corporate department, and a member of its technology, media & telecommunications group. Prior to joining the firm, she led global privacy teams for media and entertainment companies for over a decade and most recently served on the privacy leadership team for Warner Bros. Discovery. Her practice focuses on privacy and data security, delivering comprehensive expertise around data-related risk and compliance.

Julie Rubash is GC and CPO for data privacy software company Sourcepoint, where she coordinates legal efforts and ensures that the product suite innovates and expands to meet the demands created by the changing regulatory landscape. Rubash brings over 15 years of legal experience, both at law firms and as internal counsel in the media, technology and advertising sectors. Prior to joining Sourcepoint, she served as vice president of legal at advertising platform Nativo.