Bloomberg Law®

bloombergbna.com

Behavioral Advertising

INSIGHT: Fear of Brave? An Analysis of GDPR Challenges to Behavioral Advertising

BY SUNDEEP KAPUR AND MATTHEW SAVARE, LOWENSTEIN SANDLER LLP

On September 12, 2018, Johnny Ryan, Chief Policy and Industry Relations Officer at Brave Software, submitted a complaint to the Irish Data Protection Commission seeking to trigger, for the first time, an EU-wide investigation into online behavioral advertising (OBA). The complaint primarily focuses on real-time bidding (RTB), the process often used within the digital advertising industry to carry out OBA. The complaint alleges that (i) OpenRTB, the widely-used technical protocol for RTB promulgated by IAB Technology Laboratory, constitutes a ''mass data broadcast mechanism'' that violates the General Data Protection Regulation (GDPR), (ii) there are no technical measures or adequate controls to support data protection during the RTB process; and (iii) legitimate interest can never be a valid legal basis in the context of widely-broadcast RTB requests. (A companion complaint filed with the UK Information Commissioner's Office contains virtually identical allegations.)

I. Backstory

Digital advertising—particularly OBA—has been a lightning rod for criticism from privacy advocates. OBA is the serving of relevant and targeted advertisements to individuals based on information collected regarding their interactions with content on digital properties. Such information is collected via cookies, pixel tags, software development kits, and/or application program interfaces (APIs), depending on the type of digital property (*e.g.*, website or mobile application), and is utilized in the RTB process.

RTB facilitates ''programmatic'' (or automated) buying or selling of digital advertising. At a high level, RTB works as follows: a company (in industry parlance, a ''Publisher'') owns or controls available ad space (''Ad Inventory'') on a digital property. When a user visits the Publisher's online property, an organization such as a supply-side platform (SSP) or ad exchange will send a request on the Publisher's behalf soliciting buyers to bid on this available space on a per-impression basis. This ''bid request'' is received typically by a demand-side platform (DSP), which is an organization that connects buy-side organizations such as advertisers and agencies to a multitude of Publishers. Those advertisers and agencies analyze the bid request and then make their bids to purchase the ad impression. The winning buyer will have its advertisement displayed on the Publisher's digital property for that particular impression. This entire RTB process takes milliseconds.

Typically, the information contained in the bid request does not identify an individual by name, address, or similar data elements. Instead, the information is tied to a randomized persistent identifier or ''user ID'' (*e.g.*, a string of random characters used to ''identify'' a device).

The GDPR defines ''personal data'' broadly and likely encompasses such online identifiers. Thus, many organizations engaging in RTB are presumably within the scope of the GDPR. Given that bid requests are sent to multiple organizations, many of which are not directly interfacing with the user, this complex supply chain presents challenges for obtaining consent (or establishing a legitimate interest), providing transparency and choice, and controlling against unauthorized or unlawful processing.

II. OpenRTB Protocol

The gravamen of Ryan's complaint, which relies heavily on an accompanying report (the Ryan Report), is that OpenRTB is a ''mass data broadcast mechanism that gathers a wide range of information on individuals going well beyond the information required to provide the relevant adverts'' and needs (yet fails) to be GDPR-compliant. In an open letter to IAB Tech Lab regarding the latest OpenRTB specification documents, Ryan relies on a June 5, 2018 ruling from the European Court of Justice (C-210/16), better known as the ''Facebook Fan Page'' case, to attempt to demonstrate that OpenRTB *itself* falls under the ambit of the GDPR. Reliance on this case is misguided, and the complaint misstates the purpose of OpenRTB.

The Facebook Fan Page case involved a German academy that administered a fan page on Facebook. Facebook collected personal data on visitors to the academy's fan page via cookies and transmitted anonymized statistics to the academy based on the personal data collected. Although the academy had access only to these anonymized statistics, the academy could ''ask for—and thereby request the processing of—demographic data relating to its target audience, including trends in terms of age, sex, relationship and occupation, information of the lifestyles and centres of interest . . . [and] information on the purchases and online purchasing habits of visitors to its page.'' Since the academy requested Facebook to process personal data based on the above parameters, and even though it had access only to the anonymized statistics (and not the underlying personal data), the court considered the academy a joint controller with Facebook for such processing.

Unlike the academy in the Facebook Fan Page case, OpenRTB is merely a technical protocol; it does not request or direct any organization to process personal data. Although the protocol contains certain fields that digital advertising companies may populate with data considered ''personal data'' under the GDPR, OpenRTB does not require the inclusion of such data in a bid request nor does it determine the purpose or means by which such data shall be used. Rather, OpenRTB's purpose is to allow organizations to (1) broadcast bid requests from supply-side sources to demand-side sources, (2) collect bids in response to such bid requests, (3) provide notification to the winning bidder, and (4) transmit advertisements for display to individuals.

Other than the data required to satisfy the above objectives, OpenRTB is agnostic regarding the types of data collected by organizations. Notwithstanding, the Ryan Report erroneously alleges that the OpenRTB specification documents ''reveal that every time a person loads a page on a website that uses real-time bidding advertising, personal data about them are broadcast to tens—or hundreds—of companies.'' The specification documents reveal that OpenRTB does not require any personal data be included in a bid request. Although certain personal data may be found in a typical bid request, it is included only at the discretion of the particular organizations implementing the OpenRTB protocol.

Claiming that OpenRTB violates the GDPR—because organizations can use it in an unlawful manner—is no different from claiming that HTTP itself, the rules upon which OpenRTB runs, also violates the GDPR. HTTP is a set of technical rules used by browsers to communicate with servers in order to receive or transfer data over the web. HTTP is used for virtually every request made on the web, and the amount of data being ''broadcast'' through HTTP is beyond comprehension. To be sure, HTTP can be used in numerous privacy-intrusive ways. For example, organizations can use HTTP requests to drop invasive first or third-party cookies or redirect users to websites that use malware to access computers. However, few would argue that HTTP is a ''mass data broadcast mechanism'' violating the GDPR. Like OpenRTB, HTTP does not gather data on individuals or require such collection; it simply provides the framework and technical means for requests to be sent between parties.

The CNIL, the French privacy regulatory body, adopted similar reasoning in its recent guidance regarding blockchain, stating, ''A blockchain is not, in itself, a data processing operation with its own purpose: it is a technology which can serve in a diverse range of processing operations.'' More broadly, the CNIL made clear that, ''. . .the GDPR does not aim at regulating technologies *per se*, but regulates how actors use these technologies in a context involving personal data.'' The same rationale applies to OpenRTB.

III. Protecting Personal Data

Ryan's complaint also alleges that RTB does not allow participating organizations to ''control the dissemination of personal information once broadcast (or at all).'' He claims that the digital advertising industry has built no adequate controls to enforce data protection among the many companies that receive data. Such allegations, however, ignore the various administrative, technical, and physical measures implemented by organizations to safeguard personal data within the digital advertising ecosystem.

The digital advertising industry has cooperated with IAB Europe to create the Transparency and Consent Framework (TCF), which requires participating Publishers to integrate a user interface into their website or mobile application that enables individuals, at the point of data collection, to:

- view the organizations that may receive their personal data and the purposes for which they process such data;
- give or withdraw consent on a purpose-by-purpose or organization-by-organization level; and
- link to each organization's privacy policy for more information about their processing activities (including how to object to any claimed legitimate interests).

After an individual makes his or her consent choices, which can be updated at any time, a consent string is attached to each OpenRTB bid request. The consent string signals to organizations if they have consent and, if they do, for what purposes. When a bid request is broadcast, Publishers can signal which specific downstream organizations are allowed to process the personal data in such request, for what purposes, and whether organizations may rely upon legitimate interest as a legal basis for such purposes. Through these controls, individuals have increased transparency and control to make decisions regarding how organizations may process their personal data.

Apart from the TCF, there are also impression-level technical controls that organizations can and have taken in cases where consent is not granted or is unknown. For example, where exchanges have detected in the consent string that no consent has been granted to a particular DSP to receive a bid request (or where the consent status is unknown), the exchanges may do any combination of the following:

- avoid sending the bid request to that DSP;
- remove or mask OpenRTB fields that may contain personal data, such as IP address, user agent string, and user ID;
- withhold user sync requests; and/or
- remove personal data fields from any impression-level logs.

Despite the safeguards described above, the complaint criticizes the TCF for allowing organizations to transfer personal data provided they have a ''justified basis'' for concluding that the recipient has a valid legal basis to process such data.

However, the TCF's ''justified basis'' standard is consistent with the GDPR. Where a controller is sending personal data to another separate controller (*e.g.*, not a joint controller relationship), the GDPR does not obligate the transferor to *ensure* that the transferee has a valid legal basis for use of the personal data. Rather, the GDPR requires the transferor to ensure ''appropriate security,'' including in relation to unauthorized or unlawful processing. The GDPR affords organizations a considerable degree of discretion in determining what ''appropriate security'' is, stating that the organization must implement technical and organizational measures ''appropriate to the risk'' of processing. This legal obligation is consistent with the ''justified basis'' standard adopted by the TCF.

Ultimately, Ryan's claim that there are no technical measures or controls to prevent the misuse of personal data is incorrect. The TCF provides technical measures by which individuals can express choice and gain transparency with respect to how their data is used. Furthermore, there are several impression-level technical controls that have been utilized by organizations to respect user choice and safeguard data when broadcasting a bid request.

IV. Legitimate Interest as a Valid Legal Basis for RTB Processing Activities

Ryan further claims that legitimate interest is never a valid legal basis in the context of widely-broadcast RTB bid requests. However, the determination of a valid legitimate interest requires a fact-specific assessment of whether the controller's rights are overridden by the individual's interests or fundamental rights and freedoms. In light of this balancing test, it is incorrect to claim that reliance on legitimate interest by a controller in the context of a bid request is always invalid.

With respect to bid requests and attendant data processing, there are reasonable grounds as to why legitimate interest could be used as a valid legal basis in certain instances. Digital advertising organizations have economic and consumer satisfaction interests in the wide broadcast of a bid request containing personal data. If bid requests did not contain personal data—primarily the tying of the request to a randomized user ID—there would be significantly less utility for RTB. Without using identifiers, brands would not be able to use historical data relating to a particular user ID to understand to what extent the user ID has previously engaged with its advertisements, clicked through to its website, downloaded its app, or taken other actions to signal interest in its products and services. Such a framework would result in less relevant ads for consumers, lower ad revenue for Publishers, and potentially less free content. When practiced responsibly, targeting provides an enhanced user experience and economic benefits for the entire ecosystem.

Furthermore, making bid requests available to a wider array of organizations is also pro-competitive. The chief alternative to the RTB model is the ''walled garden'' approach, which limits the display of targeted ads within the Publisher's closed ecosystem. Such a situation consolidates personal data with one Publisher and prevents organizations from serving content more attuned to consumer needs.

These interests do not justify the inclusion of *all* personal data in a bid request, because, at some point, the amount and type of personal data tips the balancing scale towards the rights and freedoms of the individual. However, Ryan misleads when claiming that bid requests ''very likely'' contain sensitive data. It is unlikely that the transmission of what an individual is watching or the individual's specific location ''alone would reveal a person's sexual orientation, religious belief, political leaning, or ethnicity.'' Further, there are contractual and technical measures (*e.g.*, advertiser matching and creative scanning) to prohibit the serving of advertisements related to sensitive topics, rendering sensitive data less valuable within the ecosystem.

In practice, the most typical personal data that may be included in a bid request includes a randomized persistent user ID (such as a user-resettable device ID), information about the device itself (*e.g.*, make, model, operating system, and user agent string), the URL or mobile application the user ID is on, IP address, and, in some instances, geolocation. With respect to the balancing test between a controller's legitimate interest and an individual's privacy rights, the broadcasting of such bid request is not particularly invasive, especially since most of the information deemed to be personal data is only so because of its connection with the randomized user ID (which is likely considered ''pseudonymous'' under GDPR).

Even if the types of personal data are relatively benign, because the personal data is being broadcast to multiple organizations in the ecosystem for multiple purposes, individuals should receive reasonable notice as to how their personal data will be used in order for a legitimate interest to be maintained. As previously discussed, organizations that broadcast and receive bid requests can utilize the TCF to provide greater notice and choice, and allow individuals to decide whether to object to any claimed legitimate interests.

V. Conclusion

The complaint's assertion that OpenRTB violates GDPR is incorrect as a matter of law because a technology itself is not a processing activity subject to GDPR; GDPR compliance is attached to each organization's specific use of such technology. Further, the complaint ignores the measures taken across the industry through the TCF and other technical means to respect individual rights and freedoms. Finally, the complaint broadly and erroneously states that legitimate interest can never be a valid legal basis in the context of widely-broadcast RTB bid requests and dismisses any case-by-case assessment required by the GDPR.

Author Information

Matthew Savare is a partner and Sundeep Kapur is an associate at Lowenstein Sandler LLP, where they practice privacy, digital advertising, blockchain, and technology law.

The views expressed in this article are those of the authors and not necessarily those of Lowenstein Sandler or its clients, or of Bloomberg Law.