Lowenstein Sandler

Client Alert

The Tech Group

November 13, 2018

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

By Sundeep Kapur and Matthew Savare[1]

On September 12, 2018, a complaint was submitted to the Irish Data Protection Commission[2] on behalf of Johnny Ryan, Chief Policy and Industry Relations Officer at Brave Software, Inc., seeking to trigger, for the first time, an EU-wide investigation into certain data practices within the digital advertising industry. On the same day, a companion complaint was filed with the UK Information Commissioner's Office[3] on behalf of Jim Killock of the Open Rights Group, a non-profit organization, and academic Michael Veale of University College London.

The complaints (the "Complaints"), which are essentially identical in nature and rely, in part, on an accompanying written report from Ryan[4] (the "Ryan Report"), allege that (i) OpenRTB and Authorized Buyers, the most widely-used real-time bidding ("RTB") protocols promulgated by IAB Technology Laboratory ("IAB Tech Lab") and Google, respectively, are "mass data broadcast mechanisms" that violate the General Data Protection Regulation (the "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 bid requests.[5]

Although this is not the first assault on behavioral advertising and real-time bidding,[6] it is the first broad one under GDPR and could have profound implications across the entire digital advertising ecosystem. Although the Complaints raise certain concerns over transparency, consumer control, data security, and accountability, many of their allegations and arguments are hyperbolic or misleading, and, in certain cases, incorrect both as a matter of fact and as a matter of law. As such, although the Complaints are helpful to crystallize and shine the light on important issues, they do not demonstrate pervasive industry-wide violations of GDPR or that a massive EU-wide assessment into RTB is warranted. Rather, specific and particularized allegations of GDPR violations should be investigated, as is the case with any other industry.

I. The Backstory

From smartphones and tablets to over-the-top platforms and social media networks, content is increasingly – and in many industries exclusively – being created and consumed digitally. Concomitant with this digital transformation in media, entertainment, and journalism has been the rapid and widespread adoption of digital advertising ("AdTech").[7] Significantly, in 2017, AdTech revenue overtook broadcast and cable television advertising revenue for the first time and became an $88 billion industry in the U.S. alone. That figure is poised to rise to $107 billion by the end of this year.[8]

Despite its prevalence, AdTech, particularly online behavioral advertising ("OBA"), has been a lightning rod for criticism from privacy advocates. OBA is the serving of relevant and targeted advertisements to an individual based on information collected regarding his or her interactions with content on one or more digital properties. Such information is often 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 utilized in the RTB process.

RTB facilitates "programmatic" (or automated) buying or selling of digital advertising and is carried out through technical protocols (e.g., OpenRTB and Authorized Buyers) implemented by various organizations. At a high level, RTB works as follows: A company (in AdTech parlance, a "Publisher") owns or controls available ad space ("Ad Inventory") on a website or other digital property. When an end user visits the Publisher's online property, an organization such as a supply-side platform ("SSP") or ad exchange will send a request on behalf of the Publisher soliciting buyers to bid on this available Ad Inventory 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

[1] 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.
[2] Ravi Naik, *Grounds of Complaint to the Data Protection Commissioner* 1, https://brave.com/DPC-Complaint-Grounds-12-Sept-2018-RAN2018091217315865.pdf.
[3] Ravi Naik, *Submission to the Information Commissioner – Request for an Assessment Notice/Invitation to Issue Good Practice Guidance Re "Behavioural Advertising"* 1, https://brave.com/ICO-Complaint-.pdf.
[4] Johnny Ryan, *Report from Dr. Johnny Ryan – Behavioural advertising and personal data* 1, https://brave.com/Behavioural-advertising-and-personal-data.pdf.
[5] Naik, *supra* note 3, at 2, 3, 12; Ryan, *supra* note 4, at 3, 5.
[6] For example, on April 8, 2010, three privacy groups filed a complaint with the United States Federal Trade Commission ("FTC") claiming that certain advertising practices, including real-time bidding, constituted unfair and deceptive business practices. In their complaint, the Center for Digital Democracy, the US Public Interest Research Group, and the World Privacy Forum requested that the FTC investigate companies engaging in behavioral advertising, enjoin them from certain types of behavioral advertising, award consumers compensatory damages, and require any real-time tracking and bidding system to take greater steps to protect the privacy and economic welfare of US consumers.
[7] We use the term "AdTech" here to describe the digital advertising industry because this is the term used in the Ryan Report.
[8] Interactive Advertising Bureau, https://www.iab.com/news/digital-ad-spend-reaches-all-time-high-88-billion-2017-mobile-upswing-unabated-accounting-57-revenue/ (last visited October 24, 2018).

such as advertisers and agencies to a multitude of Publishers. In real-time, numerous advertisers and agencies simultaneously 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 from start to finish.

In certain cases, the advertiser or agency will retain the information from the bid request to assist in creating a profile of the individual, such as inferring interests in particular categories of products, and oftentimes will utilize a data management platform ("DMP"), which integrates with different data sources, to assist in the creation and augmentation of such profiles.

Typically, the information contained in the bid request about the impression 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), such as a user-resettable iOS IDFA or Android AAID, or another randomized identifier created by a particular organization.

Though many privacy laws do not consider such online identifiers as personal data relating to an individual, the GDPR defines "personal data" very broadly and likely encompasses such online identifiers.[9] 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 end user, this complex supply chain presents particular challenges for obtaining consent (or establishing a legitimate interest[10]), providing transparency and choice, and controlling against unauthorized or unlawful processing.

We devote the remainder of this article to summarizing the Complaints and the Ryan Report, and describing and analyzing the (i) purpose of the OpenRTB protocol;[11] (ii) measures used to safeguard the disclosure of personal data to downstream RTB participants; and (iii) applicability of a legitimate interest as a valid legal basis for processing activities related to RTB.

II. The OpenRTB Protocol

The gravamen of the Complaints 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.[12] 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.[13] Reliance on this case is misguided, and the Complaints misstate the purpose of OpenRTB.

The Facebook Fan Page case involved a German academy (the "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. Though the Academy had access only to these anonymized statistics, the Academy could, "with the help of filters made available by Facebook, define the criteria in accordance with which the statistics are to be drawn up and even designate the categories of persons whose personal data is to be made use of by Facebook." For example, in addition to receiving such 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.[14]

Unlike the Academy in the Facebook Fan Page case, OpenRTB is merely a technical protocol implemented by organizations to carry out the RTB process; it does not request or direct such organizations to process personal data. Although the protocol allows organizations to include personal data in a bid request, OpenRTB does not mandate the inclusion of such personal data nor does it determine the purpose or means by which such personal data shall be used.

Specifically, its purpose is to allow organizations to carry out the following objectives in a standardized way:

- Broadcasting of bid requests from supply-side sources (e.g., SSPs) to demand-side sources (e.g., DSPs);
- Collection of bids in response to such bid requests;
- Sending of "win" notifications to winning bidders; and
- Transmission of advertisements for display to individuals.[15]

Other than the data that is required to satisfy the above four objectives, OpenRTB is agnostic regarding the types of data collected by implementing organizations.[16] In this way, OpenRTB functions similarly to other web-based protocols. 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." In an Appendix, the Ryan Report presents types of personal data, which, when available, are purportedly broadcast in an OpenRTB bid request. Such personal data allegedly includes what an individual is reading or watching, a unique identifier, an IP address,

[9] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 (L 119) 111 [hereinafter *GDPR*].

[10] Under the GDPR, a controller's purposes for processing personal data must be assigned a "legal basis." The GDPR provides six different legal bases to choose from, the most applicable to the RTB context being (i) the individual has "given consent to the processing of his or her personal data for one or more specific purposes" or (ii) the processing is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party . . . ." *GDPR*, 118-119.

[11] A discussion of Google's Authorized Buyers protocol is beyond the scope of this article.

[12] Naik, *supra* note 3, at 2-3.

[13] Johnny Ryan, *Re: feedback on the beta OpenRTB 3.0 specifications*, https://brave.com/iab-rtb-problems/feedback-on-the-beta-OpenRTB-3.0-specification-.pdf.

[14] Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH ECLI:EU:C:2018:388, para. 36-39.

[15] IAB Technology Laboratory, *Reference Model*, OpenRTB Specification 3.0, https://github.com/InteractiveAdvertisingBureau/openrtb/blob/master/OpenRTB v3.0 FINAL DRAFT.md (last visited October 24, 2018).

[16] Id.; *Specification*.

a geographic location, a list of the individual's interests, gender, date of birth, and supplemental data provided by data brokers.[17]

To substantiate this claim of widespread data transmission, the Ryan Report cites AdCOM Specification v1.0.[18] Such reliance is misplaced. A review of the AdCOM specification reveals that OpenRTB does not require any of the personal data listed in the Complaints be included in any bid request. Further, none of the data actually required by OpenRTB to be included in a bid request would likely be considered personal data under the GDPR, since such data relates primarily to what technical information is needed to display the advertisement properly (e.g., if the ad contains text, images, or video; the URL where such assets are located; and the destination URL when an end user clicks on a link within the advertisement).[19] Although a certain subset of the personal data listed in the Ryan Report may be found in a typical bid request, it is included only at the discretion of the particular organizations implementing the OpenRTB protocol. The AdCOM specification deems the inclusion of such data in a bid request as optional with the exception of user ID, which is listed as recommended.[20]

Thus, claiming that OpenRTB violates the GDPR – because organizations can use it in an unlawful manner – is no different from claiming that the Hypertext Transfer Protocol ("HTTP") itself, the rules upon which OpenRTB runs, also violates the GDPR. HTTP is a set of technical rules used by a browser to communicate with servers in order to receive or transfer data (e.g., webpages, files, emails, credit card applications, surveys, browser information, etc.) over the web in the form of "requests." Since HTTP is used for virtually every request made on the web, the amount of data being "broadcast" through HTTP is beyond comprehension. And, to be sure, HTTP can be used in numerous privacy-intrusive ways. For example, an organization can use HTTP requests to drop invasive first or third-party cookies, redirect users to websites that use malware to access a computer, or serve phishing sites to gain unauthorized access to an individual's financial details. However, few would seriously 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 as directed.

The CNIL, the French privacy regulatory body (or "supervisory authority"), adopted a similar line of thought in its recent guidance regarding blockchain technology, 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."[21]

Finally, the Ryan Report calls for the OpenRTB protocol to be amended so that fields containing personal data are no longer allowed in a bid request at all.[22] However, this proposal needlessly stifles technological development out of fear of bad actors and shifts legal obligations to the protocol level, rather than the organization level, which has no basis in the GDPR. Technology is a tool used by organizations to innovate and, like all things, has the potential for abuse. It is the organization's burden to use technology responsibly and in compliance with all laws.

In sum, the Complaints and the Ryan Report allege that the OpenRTB technical protocol itself violates the GDPR. OpenRTB is not, however, a processing activity. The GDPR applies only to the *use* of personal data by organizations. Although OpenRTB facilitates such processing, it is the organizations implementing the protocol that may be governed by the GDPR.

III. Protecting Personal Data in the RTB Environment

The second core allegation of the Complaints is that RTB does not allow participating organizations to "control the dissemination of personal information once broadcast (or at all)."[23] The Ryan Report claims that "RTB establishes no control over what happens to these personal data once an SSP or ad exchange broadcasts a 'bid request.' Even if bid traffic is secure, there are no technical measures that prevent the recipient of a bid request from, for example, combining them with other data to create a profile, or from selling the data on. In other words, there is no data protection." The Ryan Report goes even further by claiming that "despite the grace period leading up to the GDPR, the AdTech industry has built no adequate controls to enforce data protection among the many companies that receive data."[24] These broad, conclusory allegations ignore the various administrative, technical, and physical measures put in place by organizations – at significant expense – to safeguard personal data within the digital advertising ecosystem and the ongoing efforts to expand and improve such measures.

Compliance with GDPR is complex in any industry. Such complexity is exacerbated in AdTech due to its incredibly complicated supply chain,[25] which includes numerous parties – many of which are intermediaries – in the RTB process (e.g., Publishers, SSPs, DSPs, agencies, advertisers/brands, trading desks, DMPs, ad servers, ad networks, ad exchanges, etc.). Because most of these market participants are downstream from the Publisher, it is difficult to establish a relationship with the end user. Thus, one of the biggest challenges vexing the AdTech industry with respect to GDPR (and, soon, other laws like the California Consumer Privacy Act of 2018) is providing the requisite level of transparency and control to individuals with respect to the processing of their personal data.

Specifically, in the RTB context, when a bid request is sent downstream to these various intermediaries, end users are largely unaware of the companies to which their personal data is being broadcast, for what purposes, and how to object to (or withdraw consent for) such processing.

[17] Ryan, *supra* note 4, at 4, 12-13.
[18] Id. at 12-13.
[19] IAB Technology Laboratory, *Media Objects*, AdCOM Specification v1.0, https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM v1.0 FINAL DRAFT.md (last visited November 12, 2018).
[20] Id.; *Specification*.
[21] CNIL, Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data (last visited November 7, 2018).
[22] Ryan, *supra* note 4, at 7.
[23] Naik, *supra* note 3, at 3.
[24] Ryan, *supra* note 4, at 3, 5.
[25] For a useful graphic illustrating the complex ad ecosystem, see https://lumapartners.com/content/lumascapes/display-ad-tech-lumascape/.

Similarly, to the extent a downstream organization relies on consent as a legal basis, it is often not in a position to know whether the Publisher verifiably received that consent and whether the scope of consent is broad enough to cover its processing activities.

In a concerted effort to address these complexities, the AdTech industry cooperated with IAB Europe to create the Transparency and Consent Framework (the "TCF"). The TCF requires participating Publishers to integrate a user interface into their websites or mobile applications that enables end users, at the point of data collection, to:

- View the downstream organizations that may receive their personal data and the purposes for which such organizations may process the personal data;
- Give or withdraw consent on a purpose-by-purpose or organization-by-organization level; and
- Link to each organization's privacy policy to learn more about their purposes of processing and how to submit a rights request (such as the right to object to any claimed legitimate interests).[26]

Each purpose displayed within the user interface is standardized and covers the various processing activities used in the RTB lifecycle by an organization (e.g., information storage and access, personalization, ad and/or content delivery, measurement, etc.). 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. This consent string signals to downstream organizations whether they have consent and for what purposes.[27] Further, 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 or not organizations may rely upon its legitimate interest as a legal basis for such purposes.[28] Through these controls, individuals have much-increased transparency and control to make decisions regarding how organizations are allowed to 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, in instances 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, which would otherwise be sent post-impression (e.g., cookie syncing); and/or
- Remove personal data fields from any impression-level logs.

Despite these technical safeguards, exchanges – as of today – can simply ignore the consent string entirely and broadcast the bid request without restriction.[29] Likewise, an agency can receive personal data through consent and then sell it to other companies that never received consent. The Complaints mischaracterize the TCF as fundamentally flawed[30] for lacking the technical measures to prevent such activities and for allowing organizations to exercise their discretion when making legal judgments.[31]

For example, the Complaints denounce the TCF for allowing organizations to transfer personal data provided they have a "justified basis" that the recipient has a valid legal basis to process such data.[32] However, the TCF's discretionary "justified basis" standard is consistent with the GDPR. Where a controller is sending personal data to another independent controller (i.e., 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.[33] The GDPR affords organizations a considerable degree of discretion in determining what "appropriate security" is, stating essentially that the organization must implement technical and organizational measures "appropriate to the risk" of processing.[34]

Notwithstanding any safeguards the parties may take before transferring data (e.g., review of the consent string, due diligence, contractual measures, etc.), the Complaints fault the TCF for the transferee's remaining discretion to use the data for an unauthorized purpose once it has been received. The Complaints essentially argue that the TCF should have technical measures to prevent an organization's use of personal data for further unlawful and/or unauthorized purposes.[35] This is an extraordinary proposal and an unworkable standard in any industry. The TCF signals user choice when a bid request containing personal data is being broadcast.However, once the personal data has been received by an organization, it is impossible for the TCF to access each organization's systems, audit its processing of the personal data, determine whether a further use is unlawful, and then delete the data if it is.

Technology has its limits in preventing bad actors from violating the law. Under any legal framework, organizations are able to use their discretion to violate the law if they desire. The Complaints' criticisms are unavailing because it implies that if the current technological measures used in the RTB ecosystem are not capable of preventing all potential violations of the GDPR by bad actors, the RTB process itself is violative of the GDPR. Like its argument regarding OpenRTB, the Complaints advocate shifting compliance responsibilities to the protocol level and eliminating the exercise of legal judgment at the organizational level.

Overall, the Complaints' claim that there are no technical

[26] IAB Europe, *IAB Europe Transparency & Consent Framework* 13-16, http://www.iabeurope.eu/tcfdocuments/documents/legal/currenttcfpolicyFINAL.pdf.

[27] IAB Europe, *In the GDPR Global DaisyBit consent solution, what purpose does the consent string serve?*, Consent String and Vendor List Format: Transparency & Consent Framework, https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/Consent%20string%20and%20vendor%20list%20formats%20v1.1%20Final.md (last visited October 25, 2018).

[28] IAB Europe, *Technical implementation*, pubvendors.json v1.0: Transparency & Consent Framework, https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md#goals (last visited October 25, 2018).

[29] However, the TCF may soon be modified to empower participating Publishers to allow bid requests to be sent only to a defined white-list of organizations.

[30] Naik, *supra* note 3, at 5.

[31] Id. at 7 ("The Framework anticipates that those broadcasting the personal data may broadcast it to third parties, when there is no consent to do so. . . . Those broadcasting the personal data are accordingly afforded discretion to rely on a 'justified basis for relying on that Vendor's having a legal basis for processing personal data.' In turn, a data subject's consent setting could be sidestepped.").

[32] Id.

[33] *GDPR*, 118.

[34] Id. at 160.

[35] Naik, *supra* note 3, at 11.

measures or adequate controls to prevent the misuse of personal data is simply 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. Finally, the level of discretion afforded to organizations by the TCF (and RTB generally) to make legal judgments is consistent with the GDPR.

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

The Complaints broadly claim that legitimate interest is never a valid legal basis in the context of widely broadcast RTB bid requests:

> Any reliance on legitimate interests for widely broadcast RTB bid requests would be misplaced. Any such legitimate interest is not absolute and would be overridden by "the interests or fundamental rights and freedoms of the data subject which require protection of personal data." In particular, providing data subjects' personal data to a vast array of third companies, with unknown consequences and without adequate safeguards in place, cannot be justified as necessary and/or legitimate, taking into account the potential impact on the rights and freedoms of the data subjects.[36]

The determination of a valid legitimate interest requires a careful assessment whether the controller's rights are overridden by the interests or fundamental rights and freedoms of the individual, taking into account the context surrounding the collection of personal data and the reasonable expectations of the individual based on his or her relationship with the controller.[37] Given that this assessment necessitates a fact-intensive balancing of interests, it is incorrect to unequivocally state that reliance on legitimate interest by a controller in the context of a widely broadcast bid request is always invalid without analyzing the specifics of how personal data is being used in each instance.

With respect to widely broadcast bid requests and attendant data processing activities, there are reasonable grounds as to why legitimate interest could be used as a valid legal basis in certain instances. Organizations in the AdTech space have clear 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 took any other action 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 targeting is practiced responsibly, it provides an enhanced user experience and economic benefits for the entire AdTech ecosystem.

Making bid requests available to a wider array of organizations is also pro-competitive. If buy-side organizations (e.g., agencies, advertisers) wanted to deliver tailored content to individuals using personal data, the chief alternative to the RTB model is the "walled garden" approach. In the walled garden, a Publisher with access to huge sets of first-party data allows buy-side organizations to display targeted ads within the Publisher's closed ecosystem. The organizations input their parameters for their target audience and the Publisher autonomously decides whom to target on its sites (or other sites, in certain instances) and what data to collect. During this process, these organizations are reliant on the Publisher's trove of data, which it does not share, and the campaign metrics the Publisher chooses to provide. As a result, the organizations gain limited insight into potential new audiences. Neither of these approaches (anonymized bid requests or walled gardens) benefits the individual from a privacy perspective either, as data is further consolidated to a few major Publishers and the practical ability to move to other organizations that better meet their needs is diminished.

Of course, these interests do not justify the inclusion of all personal data into 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. Indeed, the Ryan Report claims, without providing any support, that "the data concerned are very likely to be 'special categories' of personal data. The personal data in question reveal what a person is watching online, and often reveal specific location. These alone would reveal a person's sexual orientation, religious belief, political leaning, or ethnicity. In addition, a 'segment ID' that denotes what category of person a data broker or other long-term profiler has discovered a person fits in to."[38]

It is highly unlikely that the transmission of what an individual is watching online or the individual's specific location "alone would reveal a person's sexual orientation, religious belief, political leaning, or ethnicity." There are a multitude of reasons why someone might be watching something online, such as for research, entertainment, travel ideas, or music interests. Similarly, there are a host of reasons why someone might be in a specific location at any given time.

Further, although it is plausible that a segment ID can contain sensitive data, bid requests typically do not contain such details. This is because exchanges and Publishers often use contractual and technical measures (e.g., advertiser matching and creative scanning) to prohibit the serving of advertisements related to more sensitive topics, such as health issues, pornography, firearms, and alcohol, rendering such sensitive data less valuable within the ecosystem.[39]

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, connection type, language, device type, JavaScript support, and user agent string), the URL or mobile application the user ID is on, IP address, and, in some instances,

[36] Id. at 12.
[37] *GDPR*, 27.
[38] Ryan, *supra* note 4, at 6.
[39] The Complaints falsely claim in a footnote that the "now notorious Cambridge Analytica are [sic] but one example of the sorts of end recipients" of personal data in a bid request." Cambridge Analytica was not able to gain access to the personal data of approximately 87 million people through RTB bid requests. Rather, Cambridge Analytica used a loophole in the Facebook API to collect data on Facebook users who installed a third-party Facebook app and the friends of such users.

geolocation. With respect to the balancing test between a controller's legitimate interest and an individual's privacy rights, the broadcasting of such a bid request is not, in itself, particularly invasive, especially when you consider that 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 the 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 bid requests (e.g., exchanges and SSPs) can utilize the TCF to provide greater and more transparent notice and choice. Similarly, the TCF allows downstream recipients of such bid requests to also provide such notice and choice in order to establish a relationship with consumers and set reasonable expectations for how their personal data shall be used. Recipients can declare the purposes for which they use the personal data, include a mandatory link to their privacy policies for further information about such purposes (among other information, such as their categories of recipients and how to submit rights requests), and allow individuals to use this information to decide whether to object to any legitimate interests relating to such purposes.

V. Conclusion

The nucleus of the Complaints, which is that the OpenRTB protocol violates GDPR, is incorrect as a matter of law, considering that 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 Complaints erroneously claim that the AdTech industry has not implemented technical or other measures to protect personal data in the context of its RTB activities. This claim ignores the measures taken across the industry through the TCF and other impression-level means to respect individual rights and freedoms. Finally, the Complaints broadly state that legitimate interest can never be a valid legal basis in the context of widely broadcast RTB bid requests and dismiss any case-by-case assessment required by the GDPR.

The content of this Client Alert was originally published by Bloomberg BNA in *Bloomberg Law* on November 9, 2018. Reproduced with permission from © 2018 The Bureau of National Affairs, Inc. (800-372-1033) www.bna.com.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

SUNDEEP KAPUR
Associate
T: 973.422.6748
skapur@lowenstein.com

MATTHEW SAVARE
Partner
T: 646.414.6911
msavare@lowenstein.com

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.