

Swedish Authority for Privacy Protection, IMY

Box 8114
104 20 Stockholm

Complainant: John Stauffer
Östgötagatan 90
116 64 Stockholm

Respondents: Google
IAB Europe

GROUNDS OF COMPLAINT

A. Introduction & Purpose of this Submission

1. We write to raise concerns with the Swedish Authority for Privacy Protection regarding the Real-Time Bidding (RTB) online advertising system used by the RTB industry (“the industry”).
2. The complainant, John Stauffer, Legal Director at Civil Rights Defenders has personal and professional interests in this complaint:
3. The Respondents are responsible for aspects of the industry that result in widespread and systemic breaches of the General Data Protection Regulation (GDPR). The Respondents are headquartered in Europe as follows:
 - 3.1. **Google Ireland** – Gordon House, Barrow St, Dublin 4, Ireland
 - 3.2. **IAB Europe**– IAB Europe, Rond-point Robert Schuman 11, 1000 Bruxelles, Belgium.
4. The purpose of the submission is to seek action by the Swedish Authority for Privacy Protection that will protect individuals from wide-scale and systemic breaches of the data protection regime by Google and IAB Europe. The complaint is supported by
 - Annex 1: A report into the industry by Dr Johnny Ryan (“**the Ryan Report**”).

- Annex 2: “Update report into adtech and real-time-bidding” of the British Information Commissioner’s Office (June 2019).
- Annex 3: Supplemental evidence from Dr Ryan on the leakage of RTB personal data to data brokers, and on the scale of RTB infringements

5. We refer to these documents as the Annexes herein.

B. Background

6. The RTB system operates behind the scenes on most commercial websites and apps. It triggers rapid, automated auctions during which technology companies that represent advertisers can compete to have their advertisements shown in the advertising space on a website or app. These RTB auctions currently operate by broadcasting personal data about the person viewing the website or app to hundreds of companies in order to solicit bids from them, as detailed in the Ryan Report. These broadcasts are known as “bid requests”.

7. The Respondents, specifically Google and the IAB, define the “protocols” (or rules) for what data can and should be provided about the person who has loaded a website or app in RTB broadcasts. The Respondents run different versions of RTB: (1) IAB RTB system is called “OpenRTB” (2) Google’s is called “Authorized Buyers”.¹ The thousands of companies in the RTB industry must abide by these rules in order to participate in the multi-billion euro RTB market.

8. The IAB and Google’s RTB systems broadcast the private things we do and watch online, and where we are in the real world,² to a vast array companies, hundreds of billions of times every day.³ Google’s RTB system is active on 13.5 million websites.⁴ IAB’s RTB system is active on countless others. There is no way of limiting what then happens to these data. IAB and Google’s RTB system is therefore a vast and continuous data breach. We refer the Swedish Authority for Privacy Protection to the

¹ Previously it was called “DoubleClick”.

² See the Ryan Report for detail of what data can be broadcast.

³ For example, one RTB auction house, called Index Exchange, conducted 120 billion auctions per day. See “IX Traffic Filter: Meeting 2020’s Business Challenges with Machine Learning”, Index Exchange, 6 August 2020 (URL: <https://www.indexexchange.com/ix-traffic-filter-meeting-2020s-business-challenges-with-machine/>, last accessed 12 September 2020). See more in Annex 3.

⁴ Doubleclick.net detected on 13.5 million websites (5,002,707 and 8,823,691 further websites associated with those websites). Data from BuiltWith.com (URL: <https://trends.builtwith.com/ads/DoubleClick.Net>, last accessed 11 September 2020).

Ryan Report for a detailed explanation of RTB, how it operates, and the data protection concerns inherent in the system.

9. There are four key and related concerns:
 - i. **First**, there are no “technical or organisational measures” such as safeguards, as required by Article 5(1)(f) GDPR, to control the dissemination of RTB personal data once it has been broadcast. The sheer number of recipients mean that those broadcasting it cannot protect against the unauthorised further processing of that data, as required by Article 5(1)(f) of the GDPR. IAB Europe acknowledged, in May 2018, that “there is no technical way to limit the way data is used after the data is received”.⁵ The failings of the Respondents’ purported safeguards is described at paragraphs 30-46 below.
 - ii. **Second**, because the IAB and Google’s RTB systems broadcast personal data without any technical safeguards, it is impossible for companies using the RTB system to provide the data subject with the information required in Articles 13 and 14 GDPR. For instance, there are no adequate safeguards to prevent these initial recipients from using the data they receive for other purposes unlawfully, or from sharing the data with any number of other companies. Indeed, there is no possible way for the controller to express all the end uses, as it is not in the controllers’ gift once that data is broadcast. Thus, the controller cannot comply with Articles 13(1)(c) and 14(1)(c) GDPR.
 - iii. **Third**, the data very often include special category data.⁶ Web pages or apps individuals use may indicate their sexuality, ethnicity, political opinions etc. Such indicators might be explicit, or effectively and easily revealed using modern analytic techniques.⁷ To this end, Appendix 3 shows that RTB data is disseminated to organisations that then produce extremely intricate profiles of individuals without the data subject’s knowledge, let alone consent. Examples

⁵ “pubvendors.json v1.0: Transparency & Consent Framework”, IAB Europe & IAB TechLab, May 2018 (URL: <https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md#liability>).

⁶ See Annex: Supplemental evidence on the leakage of RTB personal data to data brokers, and on the scale of RTB infringements.

⁷ See, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) “Profiling can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data. For example, it may be possible to infer someone’s state of health from the records of their food shopping combined with data on the quality and energy content of foods.” It should also be noted (as confirmed by the CJEU in *Nowak*) that even data, such as inferences, that relates to an individual but is inaccurate remains personal data. If this were not true, the ‘right to rectification’ could never be used.

in Appendix 3 include a data broker that used RTB data to profile LGBTQ+ people in Poland in order to influence their vote in the 2019 Parliamentary Election.

Further, individuals are unlikely to know that their personal data has been disseminated and broadcast unless they make effective subject access requests to a vast array of companies.⁸ Such a task is almost impossible for data subjects, undermining the purpose of the GDPR to afford effective and complete protection to data subjects' rights.

- iv. **Fourth**, the IAB and Google RTB systems:
 - a. gather a wide range of information on individuals going well beyond the information *required* to provide the relevant adverts;
 - b. collect and disseminate that data for a range of uses that go well beyond the purposes which a data subject can understand, or consent or object to.

The Annexes evidence that there is no legal justification for such pervasive and invasive profiling and processing of personal data for profit.

- 10. Taken together, Google and the IAB's RTB system results in widespread and systemic abuses of data subjects rights. The Swedish Authority for Privacy Protection is requested to take steps to assist with ending these abuses. The action sought by the Swedish Authority for Privacy Protection is detailed at paragraphs 67-69 below.
- 11. The Supervisory Authorities for the Respondents have also taken steps to address the breaches of the GDPR inherent in the RTB systems, as follows:
 - i. **IAB Europe** - In October 2020, the Belgian Data Protection Authority (APD) found that the IAB Transparency and Consent Framework infringes the GDPR due to lack of security, transparency, and inappropriate lawful bases.⁹

⁸ This problem is aggravated by the fact that companies are largely unknown and inaccessible to data subject as the controllers that initially collect the information rarely provide explicit information on the recipients, or even categories of recipients of information, and the recipients do not inform data subjects of the receipt of this data in line with their Article 14 obligations.

⁹ <https://www.iccl.ie/human-rights/info-privacy/apd-iab-findings/>

- ii. **Google** – In March 2019, the Irish Data Protection Authority opened an investigation into suspected breaches of the GDPR by the Authorised Buyers system for “suspected infringement” of the GDPR.¹⁰ An update to that investigation is due shortly.

12. Thus, the relevant Supervisory Authorities have opened inquiries into the RTB framework and the policies and procedures underpinning its use.

C. Policies and procedures

I. Policies and procedures

13. IAB Europe has¹¹ established the “Transparency & Consent Framework” (TCF),¹² which it purports to be a GDPR compliance measure. Google also uses the TCF, and in addition has what it purports to be a contractual safeguard. We address each in turn.

a. IAB Europe – Transparency and Consent Framework

14. IAB Europe developed and operates the TCF.
15. The TCF is predicated on the idea of collecting consent from a data subject, or notifying them of legitimate interest as the lawful basis, for all subsequent data sharing to, and processing by, the hundreds (currently 628)¹³ of companies that have registered for the TCF – and the unknowable number of additional companies that these 628 may share data with.
16. The Belgian Data Protection Authority, the lead supervisory authority for the Framework, has come to preliminary conclusions about infringements of the GDPR by the TCF. Referring to the TCF, it says that:

“The Inspection Service estimates that the approach of IAB Europe shows that it neglects the risks which may affect the rights and liberties of the persons concerned. The authorisation for continuing the negotiations with a Publisher which does not

¹⁰ Section 110 of the Irish Data Protection Act, under which the inquiry is run, concerns cases of suspected infringement.

¹¹ See reference to their memorandum of understanding on the TCF at “TCF Governance”, IAB Europe (URL: <https://iab europe.eu/tcf-governance/>).

¹² https://iab europe.eu/wp-content/uploads/2020/08/TCF_v2-0_FINAL_2020-08-24-3.2.pdf.

¹³ IAB Europe TCF Global Vendor List (URL: <https://iab europe.eu/vendor-list-tcf-v2-0/>, last accessed 5 November 2020).

comply with the applicable rules and the absence of a compliance check may affect the securement [security] of the processing operation”.

17. This finding by the Belgian APD is unsurprising. There is a fundamental flaw inherent in the design of the system. The Framework expressly recognises that once an individual's data is broadcast, the data controller (and, by implication, the data subject) loses all control over how that data is used. Indeed, the Framework accepts that even where a recipient of data is acting outside of the law it may continue to provide data to that recipient. The TCF states (emphasis added):

“If a CMP [“Consent Management Platform”] reasonably believes that a Vendor [an RTB data recipient] is not in compliance with the Specifications and/or the Policies, it must promptly notify IAB Europe according to MO procedures and may, as provided for by MO procedures, pause working with the Vendor while the matter is addressed”.

This provides discretion to the controller to continue to process and disseminate personal data, even if that controller is aware that the recipient is acting in breach of data protection regulations.

18. The IAB's own documentation attests that “thousands of vendors” can receive the data from a single RTB auction, and that “there is no technical way to limit the way data is used after the data is received by a vendor”.¹⁴
19. For this reason, the CEO of IAB Europe had written to the European Commission in 2017, a year before the launch of the TCF, to acknowledge that “it is technically impossible for the user to have prior information about every data controller involved in a real-time bidding (RTB) scenario”.¹⁵ As a result, RTB would be “incompatible with consent under the GDPR”. She requested an exception for RTB in the ePrivacy Regulation for that reason.

¹⁴ <https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md>

¹⁵ Lobbying document sent by CEO of IAB Europe to senior European Commission officials, “The EU's proposed new cookie rules: digital advertising, European media, and consumer access to online news, other content and services”, IAB Europe, June 2017. This paper was sent to European Commission DG Connect (obtained by freedom of information request). See page 3 of attachment to email at URL: <https://www.iccl.ie/wp-content/uploads/2020/10/IAB-to-Commission-email-and-attachment-26-June-2017.pdf>.

20. Nor is there any way to verify or audit what the companies receiving RTB data have done with it. The TCF policies merely suggest, but make no attempt to define, a possibility that the IAB might attempt some form of review of what these companies have done with the personal data.¹⁶ Of course, it would not be possible to uncover what had occurred in a system that widely broadcasts personal data to so many companies, hundreds of billions of times a day.
 21. Furthermore, and as detailed in a recent report by Dr Ryan, in Annex 3, the data being processed often include special category data¹⁷. The APD's preliminary finding is that:
 22. "The TCF does not provide for appropriate rules for the processing of special categories of personal data. Yet, the OpenRTB standard, governed by the TCF of IAB Europe, allows processing special categories of personal data."
 23. A further concern about TCF is that it anticipates that those receiving RTB personal data may disseminate it on to third parties, irrespective of whether a data subject used the TCF features that purport to provide a lawful basis. The TCF says that a company can share RTB data with any other at its own discretion: it can rely on what the TCF calls a "justified basis for relying on the recipient Vendor's having a legal basis for processing personal data."¹⁸ A Vendor could take a discretionary view on an unspecified "justified basis" for considering that there is a lawful ground to provide personal data to a third party, even where an individual has specifically refused consent. The TCF relies on the discretion of hundreds of businesses for whom the high speed trading of personal data is a business model. A data subject might be shown a request to opt-in to processing of their data, but whether they agree is immaterial.
 24. There is no plausible reading of the TCF that adequately addresses and protects individual rights.
- b. Google – Authorized Buyers

¹⁶ "The MO [IAB Europe] may adopt procedures for periodically reviewing and verifying a Vendor's compliance with the Policies." , in "Transparency & Consent Framework – Policies Version 2020-08-24.3.2" IAB Europe, 2020 (URL: https://iab europe.eu/wp-content/uploads/2020/08/TCF_v2-0_FINAL_2020-08-24-3.2.pdf), p. 21

¹⁷ See, <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf> and <https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf>

¹⁸ At page 21, para 18

25. Google uses the TCF system, and is a prominent IAB Member. In addition, RTB companies that wish to receive RTB broadcasts from Google must sign Google's "Guidelines"¹⁹. The Guideline raises a number of concerns.
26. Google's Guidelines shift responsibility for data protection to the 964²⁰ companies that receive broadcasts of personal data from its RTB system. Google's documentation refers to these companies "Buyers", and refers to RTB bid request data as "call out data". Under the heading "RTB Callout Data Restriction", Google's Guidelines says:

"Buyer ... must not: (i) use callout data for that impression to create user lists or profile users; (ii) associate callout data for that impression with third party data".

Under the heading "Data Protection", Google's Guidelines inform the companies receiving Google's RTB broadcasts that they must notify Google if they intend to break its rules:

Buyer will regularly monitor your compliance with this obligation and immediately notify Google in writing if Buyer can no longer meet (or if there is a significant risk that Buyer can no longer meet) this obligation, and in such cases Buyer will either cease processing Personal Information or immediately take other reasonable and appropriate steps to remedy the failure to provide an adequate level of protection.

Google's safeguard depends entirely on the discretion of almost a thousand companies, who are asked to volunteer prior information about their intentional misbehaviour to Google.

27. This passage demonstrates that Google has no control over the personal data that it broadcasts hundreds of billions of times a day. Moreover, the RTB system in Authorized Buyers, designed and controlled by Google, provides for no effective control over how that data is then used once broadcast. The only restrictions are contractual,

¹⁹ <https://www.google.com/doubleclick/adxbuyer/guidelines.html>

²⁰ A further 1,218 companies are listed on Google's "certified external vendors", which are presumably only in direct receipt of data from Google outside the European Economic Area. See "Ad technology providers", Ad manager and Ad Exchange program policies, Google (URL: <https://support.google.com/admanager/answer/9012903>, last accessed 12 September 2020), and "Certified external vendors", Third-Party Ad Serving Certifications, Google (URL: <https://developers.google.com/third-party-ads/adx-vendors>, last accessed 12 September 2020).

and it is unclear to what extent these actually are, or could be, enforced. The same is true of Google's "Google Ads Controller-Controller Data Protection Terms".²¹

28. Furthermore, even these ineffectual restrictions are caveated. For example, in the Guideline it is not clear what restrictions are imposed if a Buyer is successful with their bid, as the restrictions are only placed on unsuccessful bidders (i.e. "Unless Buyer wins a given impression, it must not: (i) use callout data for...").
29. There are therefore insufficient technical safeguards to protect personal data and special category personal data in Google's RTB system.

D. The problems: Legal concerns

-
30. The background set out above demonstrates that the processing conducted by the industry gives rise to a substantial risk of on-going infringements of the GDPR.
 31. We consider that a number of the data protection principles set out in Article 5 GDPR are engaged by RTB and the relevant policies and procedures.
 - i. *Integrity and confidentiality*
 32. The principal concern about Google and IAB's RTB protocols is that they permit personal data, and special category data, to be included in RTB broadcasts, but have no way of protecting that data against unauthorised, and potentially unlimited, disclosure and processing.
 33. Article 5(1)(f) of the GDPR requires personal data to be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."
 34. The Respondents systems do not provide adequate "integrity and confidentiality" over personal data, in particular as they are unable to safeguard against unlawful and / or authorised processing by thousands of companies that receive personal data in RTB broadcasts, and which are not prevented from further sharing that data.

²¹ <https://privacy.google.com/businesses/controllerterms/>

35. In addition, the Respondents are
- a. Unable to provide transparency about the full extent of transmission and other processing of personal data once it is broadcast.
 - b. Unable to provide a formal right to data subjects to object to the use of their data by every entity that receives their data from the RTB system, because the system is designed so that data leaks to unforeseeable parties. As such, data subjects cannot know who these parties are and cannot object to the use of data by those parties if they do not know who those parties are.
- ii. *Lawfulness and fairness of processing*
36. Article 5(1)(a) requires personal data to be processed lawfully and fairly. Article 6 delimits the circumstances in which lawful processing of personal data occurs. There are only two exceptions under Article 6(1) potentially applicable to the industry:
- i. the data subject has given consent to the processing of his or her personal data for one or more specific purposes; or
 - ii. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
37. The industry is inherently incapable of obtaining appropriate consent, as acknowledged by IAB Europe in its 2017 letter to the European Commission, referred to at paragraph 18, above.
38. 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. The

APD's preliminary finding about TCF's use of legitimate interest as a possible lawful basis for RTB confirms this:

"IAB Europe does not demonstrate that the legitimate interest prevails over the fundamental interests, liberties, and rights of the relevant person which require protection of personal data; these rights have not been balanced."

39. Further, pursuant to Article 9 of the GDPR, processing of "special categories" of personal data require explicit consent if that data has not been "manifestly made public" by the data subject and no other exception applies. Nevertheless, the TCF and the Authorized Buyers Guidelines allow the industry to process data without consent, including actual or data revealing racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership, health, sex life or sexual orientation, genetic or biometric data processed for unique identification purposes. In the absence of explicit consent for such processing or any other lawful base for the processing of such data, the practices would be in breach of Article 9 of the GDPR. To this end, the APD has noted in its preliminary findings about the TCF, the only legal basis that can be relied on to process special category data is explicit consent.
40. Furthermore, explicit consent is required where significant, solely automated decisions are made relating to an individual. The Article 29 Working Party²² identify occasions where behavioural advertising, as conducted by the industry, could be considered as having "significant effects" for the purpose of Article 22 of the GDPR. This is particularly true where vulnerable individuals are targeted with services that may cause them detriment, such as gambling or certain financial products. The lack of ability to obtain this explicit consent represents a disregard for Article 22 of the GDPR.
41. There are accordingly concerns that the industry processes personal and special category data, without valid consent. Indeed, the Framework envisages a system in which data can be disseminated and broadcast without a data subject's consent. This is

²² Supra, footnote 1, at 22: "In many typical cases the decision to present targeted advertising based on profiling will not have a similarly significant effect on individuals, for example an advertisement for a mainstream online fashion outlet based on a simple demographic profile: 'women in the Brussels region aged between 25 and 35 who are likely to be interested in fashion and certain clothing items'. However it is possible that it may do, depending upon the particular characteristics of the case, including:

- the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
- the expectations and wishes of the individuals concerned;
- the way the advert is delivered; or
- using knowledge of the vulnerabilities of the data subjects targeted.

not lawful, nor in any event can this processing of data be described as 'fair' or 'transparent'.

iii. Adequacy, relevance and timing

42. We have concerns as to whether the processing of data by the industry complies with Article 5(1)(c) of the GDPR, which requires personal data to be adequate, relevant and not excessive to the purpose or purposes for which they are processed. Google and the IAB could change the rules of their RTB systems so that no personal data are broadcast. However, as the RTB industry currently operates the number of recipients of personal data, and the potential for that personal data to be further used by the recipients, has acute detrimental consequences.²³

43. Article 5(1)(e) further requires that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. The Authorized Buyers Guideline envisages (although, owing to the lack of control, cannot guarantee) personal data being retained for 18 months. Data is therefore likely to be retained for long periods without any identifiable proper purpose.

iv. Data protection by design and default

44. RTB depends on the ability to single people out through the use of digital identifiers that are tied to devices and behaviour (which today usually relate to a single individual), or link individuals across devices and contexts. These identifiers include web 'fingerprints', which relate to the unique set-up of individuals' devices and cookies placed on devices, as elaborated in Dr Ryan's report. These identifiers are difficult for individuals to access or retrieve to manage their records with data controllers that hold their information, creating a significant imbalance, and significant barrier to data subjects being able to enforce important data protection rights such as access, erasure, objection, restriction of processing and portability.

45. This in turn highlights a broader concern relating to the overarching principle of fairness in the GDPR: controllers have easy access to identifiers to single individuals out, whereas those same individuals have no real ability to use or control those identifiers. This creates concerns, in particular, under Article 25 GDPR, data protection by design and by default, which imposes a positive obligation on data controllers to build data

²³ See for example video: Dr Johnny Ryan statement and remarks at the International Grand Committee on Disinformation and "Fake News", 7 November 2019 (<https://vimeo.com/371652420>).

- protection provisions, such as access or objection, into their processing activities and systems.
- v. *Data protection impact assessment*
46. Given the breadth of personal data and special category data involved, together with the vast array of recipients of that data, the processing is likely to result in “a high risk to the rights and freedoms of natural persons.” Accordingly, Article 35 demands appropriate data protection impact assessments. At present, so far as we are aware, no proper impact assessment has been carried out, or made public.

E. Responsibility as a controller

47. Those that organise and control the RTB are data controllers. This includes IAB Europe, for the TCF and Google for Authorised Buyers.

Legal principles

48. There is sufficient evidence to suggest that the structure organised, coordinated and encouraged by the Respondents makes those entities data controllers²⁴. A data controller is defined within the GDPR²⁵ as (emphasis added)

“the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”

49. The ECJ has consistently found that the concept of 'controller' must be given a broad interpretation²⁶. Indeed, the Article 29 Working Party guidance²⁷ confirms that control “can be found [in] complicated environments, often making use of new information technologies, where relevant actors are often inclined to see themselves as “facilitators”

²⁴ Indeed, the structure itself could be considered a “body” that defines the purposes and means of processing. However, our clients need not consider this issue further for present purposes.

²⁵ The exact same wording applied in Article 2 of the 95 Directive

²⁶ C-25/17 - *Jehovan todistajat* at [21]

²⁷ Opinion 1/2010 on the concepts of “controller” and “processor”. Adopted on 16 February 2010 (available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf)

and not as responsible controllers.” Note this applies even when these entities are integrated within a larger process, such as those of a platform.²⁸

50. Further, whether the Respondents have access to the data is irrelevant. As the ECJ has found, “the joint responsibility of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned.”²⁹
51. Any suggestion that RTB is merely a technical protocol that does not request or direct any organisation to process personal data is misconceived. Such a position would also be factually inaccurate. The structure does facilitate personal data to be processed and broadcast, as the structure and the related protocols do contain fields designed to process personal and special category data.
52. Thus, the concept of joint controllership is to be given a broad and expansive interpretation to afford effective and complete protection to data subjects.

Application of law to facts

53. Those that determine the means (RTB protocols) and purposes (involvement in the RTB system) are responsible for RTB as a joint controller. In the present case, the Respondents, by creating and determining the API specifications, and the related Consent Framework and Guidelines, are data controllers for the purposes of the GDPR. In particular:

53.1. IAB and Google’s RTB structures (comprising their RTB protocols and their respective policies) have been created and crafted without sufficient regard to individual data protection concerns. Both the IAB Europe and Google structures could – and should – be remedied to have due regard to the rights of data subject. Whether the structure is so remedied is within the IAB and Google’s control.

53.2. In the *Jehovan todistajat* case³⁰, the ECJ (Grand Chamber) found the Jehovah’s Witness Community to have responsibility as a joint controller for providing guidelines, creating maps and by keeping records about members (as distinct

²⁸ Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388 at [76-77].

²⁹ C-25/17 - *Jehovan todistajat* at [69]

³⁰ C-25/17 - *Jehovan todistajat*

from the ultimate data subjects). Indeed, the Community were said to be controllers despite not interacting with the data subject. The ECJ found it sufficient that the Community had “not only... knowledge on a general level of the fact that such processing is carried out in order to spread its faith, but that community organises and coordinates the preaching activities of its members.”

53.3. This is directly comparable to the Respondents, as those corporate entities provide guidelines, a digital map in the form of the RTB specification and have a roster of members (IAB also operates a “compliance programme” that allows members to become certified by the IAB). The Respondents also have “knowledge on a general level of the fact that such processing is carried out”³¹ in order to spread RTB and IAB / Google “organises and coordinates the [RTB] activities of its members”³² through the operation of the structure.

53.4. IAB Europe acknowledge that there is currently “no technical way to limit the way data is used after the data is received by a vendor for decisioning/bidding on/after delivery of an ad but need a way to clearly signal the restriction for permitted uses in an auditable way”³³. That inherent flaw is because of the designs of the Respondents.

53.5. IAB Europe and Google, provide policies (the TCF and Authorized Buyers Guidelines, respectively) and protocols (OpenRTB and Authorized Buyers) for users to follow and adhere to. Those guides and protocols contain an inherent and systematic data protection shortfall.

53.6. The bylaws of IAB, Inc. state that its purpose is to “develop and promote interactive advertising and marketing”, and various purposes that support that end.³⁴ The constitution of IAB Europe states that its purpose is “the promotion of the marketing and sale of interactive and other advertising and sponsoring on and through the Internet in online and interactive media”, including “The provision of support for increasing the use of advertising in interactive media”.³⁵

³¹ Per C-25/17 - *Jehovan todistajat* at [71]

³² *Ibid*

³³ “pubvendors.json v1.0: Transparency & Consent Framework”, IAB Europe and IAB Tech Lab, Draft for Public Comment, May 2018 <https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/414b8e23737209f37c018611af299003d167a270/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md>

³⁴ 3.1 of “Amended and restated bylaws of the Interactive Advertising Bureau, Inc.”, 29 September 2014 (<https://www.iab.com/wp-content/uploads/2015/05/IABBylaws20140929A.pdf>).

³⁵ Section 3 of Constitution of IAB Europe

53.7. The list of IAB General Members (the ‘inner circle’ of membership) includes key industry organisations such as Google, Amazon, Facebook, etc.³⁶

53.8. An analogy can be drawn with the concept of an ‘association of undertakings’ in EU competition law. Under Article 101(1) of the Treaty on the Functioning of the European Union (“TFEU”), decisions made by association of undertakings can be anti-competitive. While the TFEU does not define the term, the Opinion of Advocate General Leger in C-309/99 J.C.J. Wouters EU:C:2001:390 stated at §61 that “[a]s a general rule, an association consists of undertakings of the same general type and makes itself responsible for representing and defending their common interests vis-à-vis other economic operators, government bodies and the public in general.”³⁷ This description fits the IAB and the underlying principle (that companies should not be able to escape their legal responsibilities by acting through ‘arm’s length’ associations) is equally applicable in the context of data protection.

53.9. Further or alternatively, IAB Europe acts not just as an independent standard setter but as a representative / agent acting on behalf of its members. Given its distinct legal personality, it is an appropriate body to bear responsibility in a representative capacity.

54. Considering the various matters raised above, the inescapable conclusion must be that those that control the structures are acting as data controllers.

Just an open-source code?

55. Any suggestion that the Respondents are passive and benign creators of a protocols and frameworks that control RTB is misguided. They are the authoritative controllers of

³⁶ See “About IAB”, page 1 at: https://www.iab.com/wp-content/uploads/2018/05/IAB_Programmatic-In-Housing_Whitepaper_v7a.pdf

³⁷ See, for example, the approach adopted in respect of Mastercard in the context of the Commission decision and subsequent litigation on *Interchange Fees* (see, in particular, the 2007 Commission Decision in Cases COMP/34.579 MasterCard, COMP/36.518 Eurocommerce and COMP/38.580 Commercial Cards). In particular, the Commission (and the European Courts) rejected an argument that the association of banks, represented by the MasterCard companies, could escape liability for the rules enacted by the association by outsourcing decision-making to the MasterCard bodies. They were not permitted to evade by ‘outsourcing’ their responsibilities in this manner. The representative MasterCard bodies, as well as the member banks, could all be held responsible for the anti-competitive effects of the rules enacted by the payment organisation.

that structure and as such, are data controllers for the purposes of the GDPR.³⁸ Any suggestion that finding the Respondents to be data controllers would have a “chilling effect on the development of open-source compliance standards that serve to support industry players and protect consumers”³⁹ would be misconceived. In particular:

55.1. The RTB Protocols and related Frameworks and Guidance go beyond merely providing an open-source standard. Rather, those participating in the RTB industry are required to use the means dictated by the Respondents to be able to participate in RTB. There is no possibility of deviating from those systems if an actor wishes to work with RTB. Thus, the Respondents determine the means and purposes of RTB and act as joint controllers of those systems.

55.2. The RTB Protocol has a widespread and significant detrimental effect on data subjects’ rights. The only actors with capacity to change that system is IAB and Google. As the CJEU has consistently found, an expansive interpretation of “joint controllers’ is required to ensure the “effective and complete” protection of data subjects⁴⁰. Without such an interpretation, data subjects’ rights would not be adequately protected.

55.3. In contrast to most open-source protocols, RTB results in widespread and systemic breaches of the GDPR. No other open-source protocol results in human rights abuses on this scale. If they did, those responsible for those human rights abuses should be responsible to remedy the breaches they have created.

56. Thus, the Respondents are able to and responsible for remedying the widespread human rights abuses caused by their protocols.

Conclusions

57. We accordingly seek the Swedish Authority for Privacy Protection to take action on the governing frameworks and the structure of the RTB system itself. Without such action,

³⁸ For example, see the forthcoming awaited case *Fashion-ID* (C-40/17), see also *Wirtschaftsakademie* (C-210/16) where the Court confirms that entities can be data controllers without ever seeing processing of personal data.
<http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d0f130da9586a3c28d9a44d98a73e6e8b2173732.e34KaxiLc3eQc40LaxqMbN4Pb3iPe0?text=&docid=202543&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=318350>

³⁹ <https://iabeurope.eu/all-news/iab-europe-comments-on-belgian-dpa-report/>

⁴⁰ See, *Google Spain, Weltimmo, Schrems, Wirtschaftsakademie and Jehovan todistajat* etc.

the individual actors that utilise and rely on the RTB structure will continue to act in breach of data protection principles, to the detriment of data subjects as a whole. Indeed, those companies face an unenviable choice; rely on the illegality latent in the structure or do not participate in Europe's RTB industry. The Swedish Authority for Privacy Protection can cure this legal deficit through an audit on the flaws and take enforcement action to ensure they are remedied.

58. In circumstances where a body is at least potentially a data controller (i.e. a 'putative' data controller) the Swedish Authority for Privacy Protection has adequate powers to take appropriate regulatory action. Without prejudice to this, the Complainants consider that, in light of the CJEU's decision in *Tietosuoja*⁴¹, the Respondents are in fact (joint) data controllers.

F. Jurisdiction

59. The Swedish Authority for Privacy Protection has jurisdiction over the activities raised in these submissions and described in the Ryan Report (see Art 55 GDPR and Chapter 1, § 5 of the Swedish Act (2108:218) on supplementary provisions to the EU General Data Protection Regulation).

i. Processing of personal data

60. Article 4 of the GDPR states that "personal data means any information relating to an identified or identifiable natural person." This includes "an online identifier" where it allows an individual to be identified, directly or indirectly. The European Court of Justice has confirmed that IP addresses can constitute personal data.⁴² Furthermore, "pseudonymised" personal data will still be treated as personal data.

61. The dissemination and broadcasting of a data subject's personal data during the RTB process involves the processing of personal data, including IP addresses or more granular personal data such as location.

ii. Complainants

⁴¹ Like the Jehovah's Witness Community in that case, the IBA is the standard setter, exerting influence on the way in which data is processed.

⁴² Case C-582/14 *Breyer*

62. Complaints are John Stauffer, Legal Director, Civil Rights Defenders, Stockholm, Sweden.

iii. Respondents

63. Pursuant to Article 3 GDPR, the GDPR will apply to data controllers outside the EU where their processing relates to monitoring the behaviour of data subjects in the EU.

64. The industry acts to offer adverts to those within the relevant territory. As such, the place of establishment of the various companies involved is irrelevant to the scope of the GDPR and the Swedish Authority for Privacy Protection's jurisdiction.

65. Note for completeness that the lead supervisory authorities are already considering the Respondents' headquarters in Europe:

65.1. The Irish Data Protection Commissioner is considering the activities of Google

65.2. The Belgian APD has already made initial findings in respect of IAB Europe

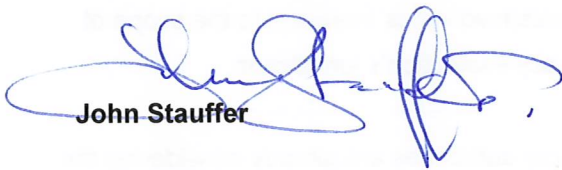
66. Given the geographical scope of the issues and companies raised in this complaint, it would be appropriate for supervisory authorities to consider this issue in unison as RTB effects all users of the internet. We accordingly invite the Swedish Authority for Privacy Protection to (1) refer this complaint to the lead supervisory authorities, namely the Irish DPC for Google and the Belgian APD, who are already conducting an investigation into the Respondents' compliance with the GDPR; and (2) liaise with other national supervisory authorities with a view to launching a joint investigation pursuant to Article 62 of the GDPR.

G. Next steps

67. The activities described above are on such scale and complexity that anyone at any time could be affected. It affects individuals, including vulnerable persons, in all walks of life, all across the EU. We therefore invite the Swedish Authority for Privacy Protection to refer this complaint against IAB Europe, and Google, to the relevant Lead Supervisory Authorities in Belgium and Ireland, who at the time of this complaint are undertaking an investigation and to liaise with their counterparts in other Member States to conduct a joint investigation pursuant to Article 62 of the GDPR.

68. We reserve the right, if appropriate, to supplement this complaint with further evidence and argument as necessary. In the meantime, if we can be of any further assistance, please do not hesitate to contact us.
69. We would be grateful if you could keep us updated on the steps taken in response to this submission, in accordance with Article 77(2) of the GDPR.

Date: 25 March 2021


John Stauffer