Select Committee on Democracy and Digital Technologies
House of Lords
London SW1A 0PW

6 January 2020

Evidence regarding "real-time bidding"

I represent Brave, the private web browser. Brave's CEO invented JavaScript, and co-founded Firefox. Brave is headquartered in San Francisco, and has an office in London.

1. Real-time bidding causes a leakage of information about voters that exposes them to the hazard of profiling and micro-targeting.

Disinformation is possible because of what happens almost every time you load an ad-supported website. When a webpage loads, data about your interests is broadcast to tens or hundreds of companies.[1] This lets technology companies representing advertisers compete for the opportunity to show you an ad.

Here are the kind of things about that you can be included in these broadcasts: your – inferred – sexual orientation, political views, religion, health conditions, etc.[2] What you are reading, watching, and listening to[3] - which allows all the foregoing to be inferred in any case - and where you are at that moment.[4] And they include unique ID codes that are as specific to you as is your social security number, so that all of this data can be added to dossiers about you.[5] I attach examples of this.

---

[1] For an overview of this process, see "Regulatory complaint concerning massive, web-wide data breach by Google and other "ad tech" companies under Europe's GDPR", Brave, 12 September 2018 (URL: https://brave.com/adtech-data-breach-complaint/). See additional evidence at https://brave.com/rtb-evidence/.

[2] See Google's RTB "Publisher Verticals" list, which is referred to in several contexts from the Google Authorized Buyers Proto (URL: https://developers.google.com/authorized-buyers/rtb/downloads/publisher-verticals); see also IAB OpenRTB "content taxonomies" list, which is referred to in several contexts in the IAB OpenRTB AdCOM API (https://www.iab.com/wp-content/uploads/2017/11/IAB_Tech_Lab_Content_Taxonomy_V2_Final_2017-11.xlsx).

[3] See "Examples of data in a bid request from IAB OpenRTB and Google Authorized Buyers' specification documents" (URL: http://fixad.tech/wp-content/uploads/2019/02/3-bid-request-examples.pdf), evidence submitted to the Irish Data Protection Commission, and UK Information Commissioner's Office, 12 September 2018 and 20 February 2019.

[4] See "Object: geo" in AdCOM Specification v1.0, Beta Draft", IAB TechLab, 24 July 2018 (URL: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md); and "Hyperlocal object", "Point object", "HyperlocalSet object" in Authorized Buyers Real-Time Bidding Proto", Google, 23 April 2019 (URL: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide).

[5] See "Object: user" in AdCOM Specification v1.0, Beta Draft", IAB TechLab, 24 July 2018 (URL: https://github.com/InteractiveAdvertisingBureau/AdCOM/blob/master/AdCOM%20v1.0%20FINAL.md); "hosted_match_data", "google_user_id", and "UserList object" in Authorized Buyers Real-Time Bidding Proto", Google, 23 April 2019 (URL: https://developers.google.com/authorized-buyers/rtb/realtime-bidding-guide).

This process is known in the online advertising industry as "real-time bidding" (RTB hereafter). As the attached examples show, the data broadcast widely by the RTB system is perfect fuel for micro-targeted disinformation, and there is no control over what companies do with it. It is by far the largest data breach ever recorded,[6] which means that any entity that wishes to profile the UK electorate can do so by simply collecting RTB "bid request" data, or buying profiles from a company that is already doing so.

2. Harmful to legitimate media, and a business model for the bottom of the web.

The data leakage and profiling made possible by RTB harms democracy in a second way: undermines the online advertising model of legitimate media, and enabling a business model for the bottom of the web.

If you read about a luxury car on The Times, and then later visit a less reputable website, you may see luxury car ads there. Companies that know you are a high value Times reader – thanks to the RTB system – show ads to you on the less reputable website at an enormous discount. They want you because you are a Times reader, but The Times does not benefit. The industry calls this "audience arbitrage".

RTB also enables fraudulent activity that further harms legitimate publishers. "Ad bots" masquerading as humans pretend to view and click on ads. Real advertisers are then charged real money, even though nobody really saw any ads.

The estimates of the cost of this "ad fraud" range from 5.8 to 42 Billion US$, diverted from legitimate publishers to the bottom of the web.[7]

Remedy

RTB both enables voter profiling and manipulation, and undermines legitimate media. Two organisations alone decide what data about people can and cannot be in an RTB broadcast. One is the "IAB", the industry's standards body, whose biggest members are Google and Facebook. The other is Google. Clearly, they should not have designed the system to operate as it currently does.

Brave's evidence[8] to regulators has triggered GDPR investigations into both of them by their lead GDPR authorities (data protection authorities in Ireland and Belgium). Regrettably, after

---

[6] For the scale of the data breach, see "Count of hundreds billions of bid request broadcasts", evidence submitted to data protection authorities in UK & Ireland (URL: https://brave.com/wp-content/uploads/2019/07/Scale-billions-of-bid-requests-per-day-RAN2019061811075588.pdf).

[7] "The impact of AI for digital advertisers", Juniper Research, May 2019 (URL: https://www.juniperresearch.com/document-library/white-papers/the-impact-of-ai-for-digital-advertisers). In the US alone, the Association of National Advertisers estimates that at least $5.8 billion of their spend is stolen by ad fraud, in "2018-2019 Bot baseline: fraud in digital advertising", Association of National Advertisers (URL: https://www.ana.net/getfile/25093).

[8] See "Regulatory complaint concerning massive, web-wide data breach by Google and other "ad tech" companies under Europe's GDPR", Brave Insight, September 2018 (URL: https://brave.com/adtech-data-breach-complaint/). See a sample of the evidence submitted to European data protection authorities so far at https://brave.com/rtb-evidence/.

over a year, we still wait for regulatory action.[9] I note that it is sixteen months since evidence from Brave and complaints about RTB were filed before the UK Information Commissioner. Despite the ICO publishing a report that vindicates every single point that we set before it, the ICO has so far not used its lawful powers of investigation or enforcement.

We urge the Select Committee to examine the RTB system in detail, and to investigate the question of enforcement. Forcing the IAB and Google to end the broadcast of any personal data in the RTB system would starve disinformation micro-targeters of data, and the bottom of the web of cash, at a single stroke.

We are at disposal of the Select Committee.

Dr Johnny Ryan FRHistS

[9] This includes Ireland and Belgian data protection authorities. See "Data Protection Commission opens statutory inquiry into Google Ireland Limited", Data Protection Commission of Ireland, 22 may 2019 (URL: https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited); and letter from Peter Van den Eynde of the Gegevensbeschermingsautoriteit to Jef Ausloos and Pierre Dewitte, 8 October 2019.