Response to the Centre for Data Ethics and Innovation Call for Evidence Consultation on online targeting

Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.

Our response to this consultation draws from two current workstreams:

- Our Data and Democracy project - this is designed to assess the interaction of election processes such as campaigning and voting with digital technologies and develop a set of principles for general use.
- Our complaint to the Information Commissioner's Office (ICO) about the GDPR breaches inherent to Real-Time Bidding (RTB) in the online advertising technology (Adtech) industry - this is also connected to a European-wide complaint and action against Adtech.

1. Harms and benefits of online targeting

The main potential benefit and harm of online targeting is its ability to affect individual behaviour, and thereby at a macro level effect societal change. However, whilst practitioners of online targeting have a vested commercial interest in consumers and businesses *thinking* that it is an effective way to change individual views or behaviour, we have found little documented evidence to support this as a reality. Studies report varying degrees of efficacy in targeting achieving its objectives, and gains are often marginal: one recent study notably found that targeted behavioural adverts generated a mere 4% more revenue for advertisers than non-targeted equivalents.[1]

There is some evidence that shows narrowly targeted online political advertising is contributing to the polarisation of democratic discourse in a harmful manner. Political actors seeking votes have always aimed to identify their audience and direct information and adverts accordingly, but online targeting ratchets this up to new levels of segmenting and individuality. When parties' messaging will only be seen by people already most likely to vote for them, it becomes less important to try and build consensus; instead, messaging becomes increasingly geared towards riling up supporters in order to drive them to the ballot box. A study by Demos has evidenced how this "riling up the base" approach can then be used to fuel a decidedly nasty kind of political engagement.[2]

The way in which online targeting currently takes place further puts individual privacy at risk, which is a significant harm. Our complaint to the ICO on real-time bidding (RTB) in

[1] NB. This finding also begs the question of who *is* profiting. Marotta, Abhishek and Acquisti, *Online Tracking and Publishers' Revenues: An Empirical Analysis*, Preliminary Draft May 2019 <https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf>

[2] Demos, *Warring Songs: Information Operations in the Digital Age*, May 2019 <https://demos.co.uk/wp-content/uploads/2019/05/Warring-Songs-final-1.pdf>

the Adtech industry identifies how data transfers take place with a complete disregard for GDPR compliance and fail to put any safeguards in place to ensure that data is processed securely.[3] Every time a person visits a website that uses RTB systems, intimate personal data about them and what they are viewing is broadcast in a “bid request” to tens or hundreds of companies, to solicit bids from potential advertisers’ for the opportunity to show an ad to this specific visitor. The data can include people’s exact locations, inferred religious, sexual, political characteristics, what they are reading, watching and listening to online, and unique codes that allow long term profiles about each person to be built up over time. This data sharing occurs hundreds of billions of times every day and there are no control limits over what happens to the data once broadcast. The privacy invasion it comprises is a harm which is insidious, widespread and unacceptable.

2. Operational aspects of online targeting

Broadly speaking, online targeting is used by commercial and political actors to profile individuals and market directly to them. It is focused on maximising conversion rates - i.e. streamlining information and advertising so that these are shown only to the people already susceptible to the message and therefore most likely to be swayed to “buy in” (literally or metaphorically) to a product, idea or political worldview. This ostensibly maximises cost efficiency for advertisers and is argued to give users more relevant info/ads and so an enhanced online experience. We remain unconvinced by either of these arguments.

At a granular level, the mechanics of online targeting are opaque. The basics of how RTB operates is public knowledge, but in our Adtech complaint we still have many unanswered questions over e.g. how the data flows occur and to what extent. There is a high degree of secrecy in the Adtech industry which frustrates information-gathering. We are in the process of commissioning expert reports to increase our understanding of certain aspects of Adtech, but more research and transparency in this area is vital.

In terms of online political advertising, we are currently working to gather evidence on how UK political parties profile citizens and carry out online advert targeting. We have submitted a range of Subject Access Requests (SARs) to various political actors and our findings from these will be published in due course. We also collaborated with ‘Who Targets Me’ to obtain data on how online targeting was used in the 2019 European Elections. Who Targets Me is a browser plug-in which records the political ads with which Facebook users are served - something that previously was not possible as ads disappeared without record once they had been seen by a user. Who Targets Me anonymised data can identify exactly what ads political parties are using and how they are being distributed - i.e. which particular ad versions are targeted at which particular users, on what basis and at what frequency.[4] We are currently analysing the UK data obtained in the election period and findings will be published shortly.

At an overview level, we broadly expect our SAR and Who Targets Me findings to concur with those of Carl Miller, Director of the Centre for the Analysis of Social Media at Demos, whose attempt to “reconstruct [his] data doppelganger” concluded that (1) Data brokers

[3] This complaint has also now been submitted to data protection authorities across the EU, with 15 complaints filed to date. Complaint and surrounding information/documentation available at: <https://fixad.tech/september2018/Fixad.tech>

[4] More information is available at: <https://whotargets.me/en/>

and businesses organise our personal data profiles into percentage "scores" (2) These scores often seem unrelated to and unreflective of real life characteristics and interests - and thus it is hard to see how they would be effective behavioural predictors, and (3) The process of retrieving this information is difficult and bureaucratic to the point of being off-putting.[5] These conclusions point to the inability of online targeting to achieve its stated objectives and a lack of transparency and accountability over actors operating in this sphere.

This lack of transparency is a critical operational flaw. Neither consumers nor businesses can be fully aware of the personal information that is used to target them or how it is categorised. Nor can they currently exercise any effective control over how that data is processed, including with which third-party actors it is shared. In RTB, once personal data is broadcast in a bid request, it can be stored by hundreds of adtech companies and combined with other data to build up detailed individual profiles for later bidding purposes. Tracking your data cleanly through the RTB system is an impossible task.[6]

Governance and accountability of online advert targeting is also poor. RTB is governed by the Interactive Advertising Bureau (IAB)'s Transparency and Consent Framework and Google's Authorized Buyers programme, but these do little to properly protect personal data in online ad targeting processes. Google relies on self-written guidelines that expect the companies that receive its broadcasts to inform it if they are breaking its rules[7] and the IAB knew that real-time bidding would be "incompatible with consent under GDPR" before it even launched the system.[8]

3. Regulation of online targeting

In our view, online targeting needs to be regulated. Where possible, data protection laws and frameworks should be used. The following data protection concepts have particular relevance:

Consent (Article 7 GDPR): data collection requires consent when it is not essential for a purpose or justified by some general purpose. It is unclear that utilising user data for advert targeting even on a platform like Facebook is essential; rather it is *useful* for Facebook to monetise its service. Targeting is likely to require separate consent to platform use, thus many current models of targeting may require changes to comply with GDPR.

Special category data (Article 9 GDPR): many kinds of online targeting, for instance political targeting, appear to profile people using political and religious beliefs and opinions that data protection defines as sensitive personal data. This data processing normally requires specific separate consent, except in the context of certain party campaigning. If reinforced and clarified, the special category data concept could help protect against certain abuses relating to beliefs and opinions.

[5] BBC Click Investigation, *Would you recognise yourself from your data?,* 29 May 2019 <https://www.bbc.co.uk/news/technology-48434175>
[6] See report of Dr. Johnny Ryan, Brave, affixed to our ICO complaint, fn 3 above.
[7] Google Authorized Buyers Program Guidelines <https://www.google.com/doubleclick/adxbuyer/guidelines.html>
[8] *New evidence to regulators*, 20 February 2019 <https://fixad.tech/february2019/>

Fair processing (Article 5 GDPR): this concept could be very powerful for prevention of discrimination, unfair and prejudical judgements and unexpected uses of data where 'consent' might appear to be present. Applied to algorithmic calculations and machine learning, the concept could be used to limit the more extreme and obviously detrimental uses of targeting.

Automated decision making (Article 22 GDPR): GDPR envisages transparency for significant decisions made through automated decision making. Where there are risks of detriment, there is a clear case for extending this principle to methods of online advertising so that users are given greater knowledge of how and why they are targeted.

Machine based signals for preferences: GDPR envisages signals being sent to express the users' privacy preferences rather like Do Not Track was intended to do. Such technologies could reduce the kinds of inappropriate targeting, for instance by expressing a desire not to be targeted for certain or all purposes.

Our complaint and its sister complaints in jurisdictions across the EU demonstrate that independent self-regulation has failed when it comes to regulating online targeting as it relates to RTB. The scale of concern is indicated by the number of challenges that have been brought. Compounding the self-regulation failure however, is the weak response we have encountered by data protection authorities (DPAs) struggling with how to respond to the systemic data protection failings at the heart of RTB systems. DPAs are worried about the potential negative impact of enforcing our complaint on the online advertising ecosystem, but this is itself problematic, as it does not protect individuals to have regulators be overly cautious about fully regulating. Regulators that do have authority need to be empowered to exercise this and hold industry actors and bodies to account.

One of our aims in supporting EU-wide RTB complaints is to prompt an investigation into this issue by the European Data Protection Board. Any regulation of RTB targeting needs to be pan-European. These systems operate across jurisdictions, and a patchwork of national-level regulation would not be effective: it is critical that the UK engage with EU institutions and EU-wide DPAs.

In terms of regulation of online political advertising and the targeting that entails, we suggest that regulation that focuses purely on 'cost containment' is unlikely to be truly effective, and actors other than the Electoral Commission need to be engaged, particularly the ICO. In its present constitution, the Electoral Commission is a spending regulator, limited in function and without the remit or power to address the modern landscape of online political targeting. It was needed in the early 2000s to rein in excessive spending by political parties at a time when sheer financial spending (mostly) directly increased election win likelihood, but is is a relic of the era of "floppy disks and dial up internet"[9] and no longer fully fit to address contemporary and emerging online targeting realities.

When expensive mass media ad campaigns are the chief campaigning organ in elections, it is appropriate and right to regulate election spending in order to prevent any one party artificially tipping the democratic scales in their favour by amassing a financial 'war chest'

[9] Electoral Reform Society Report, *Reining in the Political 'Wild West': Campaign Rules for the 21st Century*, 4 February 2019 <https://www.electoral-reform.org.uk/latest-news-and-research/publications/reining-in-the-political-wild-west-campaign-rules-for-the-21st-century/>

that can meet the costs of these. However, this is no longer how political advertising works. Political parties use personal data to include or exclude potential voters; they then target ads online only, and intensely, at their most likely supporters. This drives down spending by targeting only a narrow slice of the population. In addition, automated messaging is becoming both cheaper and more sophisticated, and the marginal cost of production and distribution of campaign material is reduced in digital markets due to factors such as virality. Both of these practices significantly reduce the amount of money needed to run effective political campaigns. Consequently, to regulate online political targeting effectively, we need to look beyond campaign spending.

The Election Commission has proposed introducing new reporting requirements such as increasing the granularity of spending declarations, but ORG considers this is likely to be insufficient by itself. A more holistic approach is needed. The new centre of power for effective political campaigns is information capital. What is most crucial in electoral regulation, therefore, is transparency and accountability over parties' use of personal data for online targeting.

Transparency can be supported, to a degree, by initiatives such as Facebook's online ad library. The limited data that Facebook provides, however, still allows shady individuals who pay for ads online to conduct 'astroturf' campaigns hidden behind shell companies - as in the case of "Outreach Groups" during the UK's referendum on EU membership in 2016.[10] A more holistic regulatory approach is needed. Regulation needs to hold the political actors that use online advertising - and the online platforms that facilitate them - accountable as to their sources of personal data and how their targeting works. It also needs to take into account the responsibilities of different actors such as third-party campaign groups and data brokers. It needs to recognise that political opinions have sensitive personal data status under the GDPR, and therefore require a high level of protection.

4. Developing technologies, issues and legal frameworks affecting online targeting

GDPR should do more to govern online targeting, but enforcement is currently lacking. Our ICO complaint on AdTech is now Europe-wide, so its outcome could have a significant impact on the way online targeting in RTB systems operates.

There is also increasing academic interest in the economic impacts and choices of RTB, so we expect to see further research in this area.

ORG is currently monitoring how digital technologies might develop.

[10] New Statesman, *Brexit astroturfing: did fake grassroots groups help swing the EU referendum?*, 7 August 2018 <https://www.newstatesman.com/politics/brexit/2018/08/brexit-astroturfing-did-fake-grassroots-groups-help-swing-eu-referendum>