Response to Centre for Data Ethics and Innovation: Review of online targeting

Dr Anya Skatova[1], Dr Philipp Lorenz-Spreen[2], Professor Stephan Lewandowsky[1], Dr Mark Leiser[3], Dr Stefan Herzog[2]

1. School of Psychological Science, University of Bristol, UK
2. Max Planck Institute for Human Development, Berlin, Germany
3. Leiden Law School, Leiden University, The Netherlands

Contact the authors - anya.skatova@bristol.ac.uk, lorenz-spreen@mpib-berlin.mpg.de, stephan.lewandowsky@bristol.ac.uk, m.r.leiser@law.leidenuniv.nl, herzog@mpib-berlin.mpg.de

In this submission, we have responded to Questions 1 and 3. We respond as individuals acting in a professional capacity, informed by our research and knowledge of the evidence base. Throughout, we present evidence-based examples to support our position. Our submission should not be interpreted as representing the views of our respective institutions.

Summary

- When designing regulation for the digital environment, the starting premise should be that *everyone* is vulnerable ("pervasive vulnerability"). As everyone is subjected to targeting, approaching this as a problem that only affects particularly vulnerable groups or people is inadvisable. (Question 1)
- As data is increasingly collected and inputted into more complex user profiles, the risk of harm increases over time in correlation with the technology and the associated efficiency of the targeting. This applies regardless of the method of online delivery. (Question 1)
- The legal framework should require online platforms to give users: 1. Clear and comprehensive information about online targeting; and 2. Transparent opportunities to determine the circumstances when they are or are not willing to accept online targeting. (Question 3)
- Any regulatory or legislative response to targeting (e.g. bans; requirements on the design of online platforms) must mandate transparency, accountability and user empowerment and protection. (Question 3)
- Any regulatory framework should apply equally to commercial and political advertising. (Question 3)

Question 1: What evidence is there about the harms and benefits of online targeting?

Summary: Personalization is indispensable for navigating the vastness of the online and offline world, and our choices are context dependent. However, sophisticated profiling techniques put us at risk of exploitation online. The notion of '*pervasive vulnerability*' can help us understand the harms of targeted content and advertising.

Online targeting has clear benefits. Users see ads that are relevant and useful to them and are spared exposure to irrelevant information. Companies and political parties can target groups of people who are likely to use and enjoy their products and services. However, when successful, targeted advertising may induce and sustain unnecessary consumption and may create opportunities for political manipulation.

> **Example**: YouTube's recommender system presents users with other videos they might enjoy. But this can lead to increasingly radical content: within a few clicks, users can be directed to extremism content (e.g. right wing or Islamist).[1]

Conventional opposition to online targeting often appeals to compromised agency and autonomy. That is, targeting is seen to infringe on people's free will or free choice. However, we all make decisions within an environment or context that prompts, nudges and shapes our decision-making to some degree, whether online or not, and whether we like it or not.

> **Example**: A person does not walk into McDonald's to order "326.8 ml" of a beverage to match the extent of their thirst: we cannot quantify our preferences and needs in this manner. Instead, the choice is between a small, medium, or large beverage, whatever those sizes may be. And if the available choices change, our preferences change. This context-dependence of our choices is inescapable and hence we must accept that *someone* is providing that context. There is no decontextualized 'free choice' that we can exercise.[2]

In the online environment, the available (or observable) choices we have, and information that we see, are increasingly cultivated by sophisticated and intelligent profiling techniques. These can exploit a detailed understanding of our digital footprint, such as 'likes' and 'dislikes'.

> **Example:** Knowledge of 300 Facebook 'likes' is sufficient to infer a person's personality with greater accuracy than that person's spouse.[3]

---

[1] Schmitt, J B, Rieger, D, Rutkowski, O and Ernst, J. Counter-messages as Prevention or Promotion of Extremism?! The Potential Role of YouTube Recommendation Algorithms, *Journal of Communication* **68**(4), 780-808, 2018, https://doi.org/10.1093/joc/jqy029

[2] Stewart, N, Chater, N. and Brown, G. D. A., Decision by sampling, *Cognitive Psychology* **53**(1), 1-26, 2006, https://doi.org/10.1016/j.cogpsych.2005.10.003

[3] Youyou, W, Kosinski, M and Stillwell, D, Computer-based personality judgments are more accurate than those made by humans, *Proceedings of the National Academy of Sciences* **112**(4), 1036-1040, 2015, https://doi.org/10.1073/pnas.1418680112

[4] Hilbert, M. & López, P. The world's technological capacity to store, communicate, and compute information, *Science* **332**, 60–65, 2011, https://science.sciencemag.org/content/332/6025/60

With increasingly sophisticated technology to collect and process large amounts of data,[4] **all online users become vulnerable** – what we term here 'pervasive vulnerability'. This is because the amount of data collected about users is sufficient to infer highly personal details about them.[4] This in turn permits their targeted exploitation and manipulation. It has been shown that people find targeting more acceptable when it is based on directly accessible census data or voluntarily provided information;[5] that is, data about a person that are routinely accessible to others and are accessible to the person themselves.

Targeting becomes problematic when behavioural data are used to infer what may be unknown to the person themselves or has not been actively provided. Regardless of how data is collected, the smaller the target group, the more customized a message must be. In the extreme case, each individual sees completely different content, which can undermine or even destroy a shared reality and discourse opportunities in the online environment.

> **Example:** A person is targeted for weight-loss products based on their exercise data or the inference from 'likes' or search history of an eating disorder. The problem is exacerbated in the political domain, if manipulators can incite someone by appealing to their prejudices and biases.

Online targeting can also be problematic for democracy and economies.

> **Example:** The accessibility of arguments in a political debate is a fundamental aspect of democracy, which is undermined by targeted advertising.[6] The free marketplace of ideas is supposed to weed out bad ideas.[7] In the absence of transparency, dynamic online advertising whose messages are known only to the sender and the recipient, and therefore do not permit rebuttal, are fundamentally incompatible with a marketplace of ideas.

Considered together, these three aspects of targeting – whether data has been provided or inferred, the size of the group being targeted and the nature of the context (e.g. political, commercial) (see Figure 1 for visualisation) – making most online users vulnerable to targeting in the long run[8]. These dimensions of targeting become particularly problematic when they are being used simultaneously.

> **Example:** Political information that is based on non-public data and aimed at small audiences is highly problematic for democracy. By contrast, commercial advertising aimed at large groups of people and based on publicly-available data is likely to be less problematic.

The risks of online targeting are heightened by modern technology, like narrowing down the target group with the help of automated data collection or inferring more intimate information through machine learning[9]. This suggests that new technology enables advertisers to move further along

---

[5] https://www.vodafone-institut.de/studies/transparency-and-user-control-critical-to-success-of-big-data-3/

[6] https://fullfact.org/media/uploads/full_fact_tackling_misinformation_in_an_open_society.pdf [needs full reference]

[7] Kaufmann, C. Threat inflation and the failure of the marketplace of ideas: The selling of the Iraq war. *International Security*, **29**(1), 5-48, 2004, https://doi.org/10.1162/0162288041762940

[8] https://money.cnn.com/galleries/2010/technology/1012/gallery.5_data_breaches/index.html

[9] https://www.theguardian.com/media-network/media-network-blog/2014/sep/29/technology-changing-marketing-digital-media

the dimensions depicted on Fig. 1 (e.g., from provided to inferred data, from purely commercial to political use of the targeting) making targeting increasingly problematic for our democracy by allowing forever more precise manipulation.

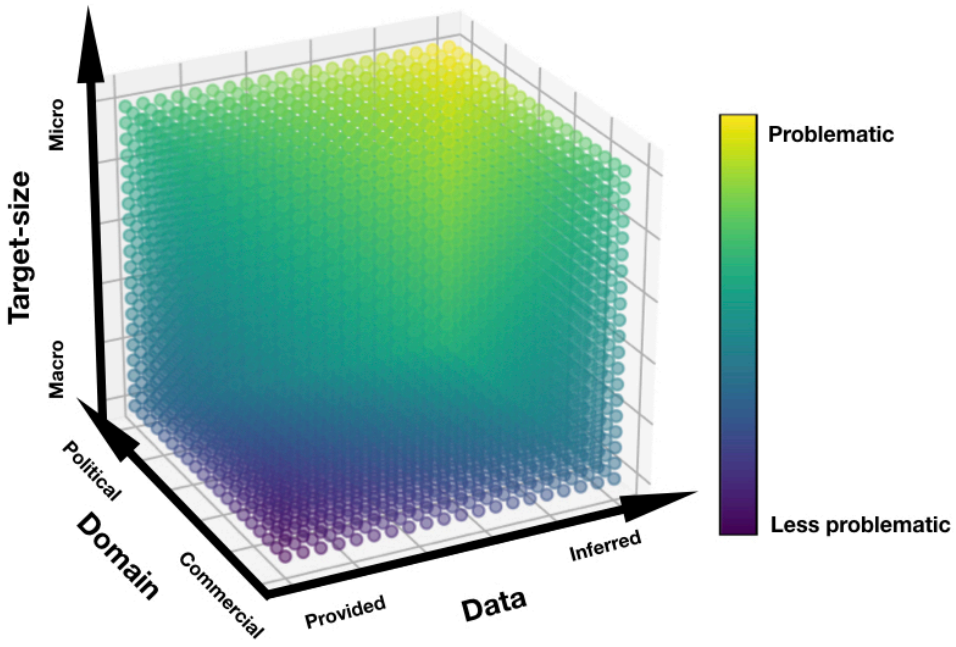

Figure 1 - Visualization of the different dimensions of vulnerability that can make targeting problematic and their additive relationship.

Question 3: Should online targeting be regulated, and if so, how should this be done in a way that maximises the benefits and minimises the risks targeting presents?

Summary

Online advertising regulation should move from self-regulation to a regulatory framework which mandates transparency, accountability and user empowerment and protection. This legal framework should require online platforms to give users clear information about online targeting and transparent opportunities to determine the circumstances when they are or are not willing to accept online targeting.

Regulators, the public and politicians are rightly concerned about how to regulate the internet. This concern must, however, be accompanied by the recognition that the internet *is* already regulated. However, this regulation is heavily dominated by corporations with little public supervision and accountability[10]. In response to demands to increase transparency and accountability, platforms have already agreed to a voluntary code of self-regulatory standards that aim to increase transparency in political advertising. Platforms have also undertaken initiatives to increase transparency and accountability.

> **Example**: Facebook has implemented an authorisation procedure for all political and issue-based advertising and requires a 'paid-for' disclaimer on all ads. However, this is limited to specific electoral events and it is not possible to track which ad was targeted to which audience. Facebook's new public repository permits users to see the number of political- and issue-based ads that were run in EU member states, along with information like aggregate advertiser expenditure and pages running each ad. Regulators, watchdogs and media will be able to take advantage of expanded access to Facebook's Application Programming Interface (API) to help increase accountability.

However, the general public needs more tools to protect themselves against online targeting. The regulatory objective should focus on what empowers the users to know why he/she is shown certain ads and to decide which ads and which information he/she finds acceptable to be used for targeting and allow to block certain campaigns.

> **Example:** If users in the real world can add their name to a 'do-not-mail' list that informs the post office not to deliver junk mail and can request telephone numbers are added to 'do-not-call' phone lists, then users in the online environment should also be empowered with the right not to be targeted by online advertisers and content.

But to be able make that decision in an informed way, online targeting needs to be transparent, with advertisers and content providers accountable for unsolicited communications users deem inappropriate. Users should be able to identify out all of the actors behind online targeting and targeted ads, and why posts appear to them which is currently not possible. This level of transparency will allow users to correct any personal data that results in inappropriate inferences

[10] Yemini, M. The New Irony of Free Speech. *20 Columbia Science and Technology Law Review*, **119**. 2018. https://ssrn.com/abstract=3247735

and allow data subjects to fully exercise their rights under the GDPR. This information should be stored and accessible, allowing for further examination in terms of transparency. Using their GDPR data portability right, users should be able to send to a regulator information about the ad, the demographics the ad targeted, and whether other users saw the same image/ad/post. Ultimately all users should be able to opt-out of any online targeting campaign they wish to opt out.

In order to ensure transparency and that democratic processes are not manipulated by those with the best technology, the regulation of online advertising must be updated to reflect the harms associated with targeted advertising. Policies implemented to regulate targeting do not need to replicate what has been previously done in the non-digital world because it is a substantially different issue regulating a medium which is still developing, and with techniques often little understood.

We suggest five changes to the regulatory frameworks:

1. Characterise all targeted online advertising as commercial communication (including political advertising) so that it is regulated in the same ways.
2. Move from purely self-regulatory frameworks to co-regulation of advertisers and platforms. The regulator should have the ability to license actors where appropriate, issue codes of practice, regulate, resolve disputes, handle complaints and issue sanctions, fines, and other forms of enforcement mechanisms against non-compliant advertisers.
3. Monitor regulatory effectiveness against three benchmarks: i. transparency, ii. accountability, and iii. the mandated integration of user control.
4. The legal framework should require online platforms to give users: 1. Clear information about online targeting; and 2. Transparent opportunities to determine the circumstances when they are or are not willing to accept online targeting[11]
5. Develop better technological solutions to both monitor exploitation of vulnerabilities by personal data and to police algorithms used by industry.[12] Online targeting is different from the analogue version, and new digital solutions are needed to regulate it due to the scale, speed and sophistication of targeting techniques.

[11] http://www.pewinternet.org/2018/11/16/public-attitudes-toward-computer-algorithms/
[12] e.g. https://arxiv.org/abs/1905.09350; https://www.nber.org/papers/w25548