# Response to Call for Evidence for the Review of Online Targeting by the Centre for Data Ethics and Innovation

**Submitted by Prof. Derek McAuley and Dr. Jiahong Chen of**
**Horizon Digital Economy Research Institute, University of Nottingham**

**14 June 2019**

1. Horizon[1] is a Research Institute centred at The University of Nottingham and a Research Hub within the RCUK Digital Economy programme[2]. Horizon brings together researchers from a broad range of disciplines to investigate the opportunities and challenges arising from the increased use of digital technology in our everyday lives. Prof. McAuley was principal investigator on the ESRC-funded CaSMa[3] project (Citizen-centric approaches to Social Media analysis) to promote ways for individuals to control their data and online privacy, the EPSRC-funded UnBias[4] (Emancipating Users Against Algorithmic Biases for a Trusted Digital Economy) project for raising user awareness and agency when using algorithmic services. Dr. Chen is a Research Fellow of Horizon, currently working on the EPSRC-funded DADA[5] (Defence Against Dark Artefacts) project, addressing smart home IoT network security, and its acceptability and usability issues; before joining Horizon, he completed his PhD on online behavioural advertising and the GDPR.
2. We are submitting this response in our personal capacity, and are happy to be contacted at derek.mcauley@nottingham.ac.uk and jiahong.chen@nottingham.ac.uk and for any part of this submission to be published.

***1. What evidence is there about the harms and benefits of online targeting?***

***1.1. What evidence is there concerning the impact - both positive and negative - of online targeting on individuals, organisations, and society? In particular:***

***1.1.1. Its impact on our autonomy***

3. Online targeting may impose serious impact on individual autonomy mainly from three aspects: First, it runs counter to the idea of informational self-determination. A large part of the current online targeting practices, especially those involving real-time bidding or programmatic trading, do not allow sufficient individual control over how personal data is collected, circulated, analysed and reused.[6] Second, it undermines individual liberty by causing chilling effect on online behaviour. In the absence of transparency, online targeting may cause internet users to become self-conscious

[1] http://www.horizon.ac.uk
[2] https://epsrc.ukri.org/research/ourportfolio/themes/digitaleconomy/
[3] http://casma.wp.horizon.ac.uk
[4] http://unbias.wp.horizon.ac.uk
[5] https://www.horizon.ac.uk/project/defence-against-dark-artefacts/
[6] See Edith G. Smit, Guda Van Noort and Hilde A.M. Voorveld, 'Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe' (2014) 32 Computers in Human Behavior 15.

about being monitored or discriminated, and thus refrain from certain activities even if they are fully legitimate.[7] Third, it jeopardises the principle of equality and non-discrimination. Online targeting enables price discrimination and other forms of unfair differentiated treatment,[8] which may result not just from mistaken data and misrepresentation of the individuals concerns, but also from accurate yet uncontested, unjustified differentiation.[9] It is not for those concerned about such abuses to prove them but for those adopting them to prove they are acting responsibly.

#### *1.1.2. Its impact on vulnerable or potentially vulnerable people*

4. One's online behavioural profiles can reveal much about their potential physical and mental vulnerabilities.[10] These online targeting techniques, while possibly developed with benign intentions, may be easily repurposed for, or even accidently engaged in, subtle forms of discrimination against vulnerable people. More importantly, these techniques can be potentially employed to target individuals who are not traditionally considered with vulnerabilities but still particularly susceptible to unfavourable treatment or unjust influence. For example, there have been concerns over the potential use of online targeting data by insurance[11] and gambling firms[12] to target individuals with potential vulnerabilities.

#### *1.1.3. Its impact on our ability to discern the trustworthiness of news and advertising content online*

5. The Cambridge Analytical scandal shows how online advertising may have significant impact on our democracy, and how political messages can be disseminated effectively with online targeting.[13] Online targeting limits the exposure of individuals to a diversity of information sources representing different political positions and different degrees of reliability. The general public are thus less aware of the broader landscape that is necessary for informed decisions regarding the trustworthiness of online content. Importantly, there should be a public register of political advertising in order that the public are able to form a more holistic view of any party's manifesto.

#### *1.1.4. The impact on privacy and data protection rights of the collection, processing and sharing of data that underpins online targeting*

6. Under the GDPR and the ePrivacy Directive, as well as their UK implementations (the DPA 2018 and the PECR), the collection and use of personal data, and the use of cookies or other tracking

---

[7] See http://www.bbc.co.uk/news/uk-politics-35060064

[8] See Frederik Zuiderveen Borgesius and Joost Poort, 'Online Price Discrimination and EU Data Privacy Law' (2017) 40(3) Journal of Consumer Policy, 349.

[9] See Jiahong Chen, 'The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle' (2018) 4(1) European Data Protection Law Review 36.

[10] See https://thenextweb.com/artificial-intelligence/2018/10/15/amazons-new-patent-will-allow-alexa-to-detect-your-illness/, https://www.forbes.com/sites/haroldstark/2017/05/23/facebook-is-letting-advertisers-target-suicidal-minors-whats-next

[11] https://www.theguardian.com/money/2016/nov/02/facebook-admiral-car-insurance-privacy-data

[12] https://www.telegraph.co.uk/news/2018/06/25/gambling-firms-could-use-gps-tempt-vulnerable-customers/

[13] See Balázs Bodó, Natali Helberger and Claes H. De Vreese, 'Political Micro-targeting: A Manchurian Candidate or Just a Dark Horse?' (2017) 6(4) Internet Policy Review 3, 4-5.

techniques for online advertising purposes should be justified with the data subject's consent.[14] Also, comprehensive and comprehensible information must be provided to data subjects, who have the rights, inter alia, to object to the use of their data, to withdraw consent, and to request erasure of their data.

7. The common practices of the online targeting sector, however, do not fully comply with these requirements. Consent is often obtained on an "opt-out" basis, and sometimes required as a condition for access to the service; information about data use is hard to find and understand; there is no simple way for users to opt out of online targeting or exercise their "right to be forgotten". The complexity of the ecosystem[15] makes it even harder for data subjects to effectively exercise these rights. The requirement to engage with this process on every website is wearing and consumers stop being able to give it attention – the voluntary "do-not-track" system to enable a global default option concerning tracking has been systematically undermined by the industry and needs the regulatory backing to make it a requirement.

### *1.2. What opportunities are there for targeting and personalisation to further benefit individuals, organisations, and society?*

8. The online advertising sector has constantly claimed – or commissioned studies to support the claims – that online targeting is good for individuals (tailored ads[16] and free services[17]), for commerce (digital market[18]), and for the society (innovation and democracy[19]).

9. Our research, however, shows that most of these claims are at best highly challengeable. The claims and studies are either subject to serious methodological flaws (in terms of measuring user attitudes and market value) or misleading on the objectives (by ignoring the essence of responsible innovation and participatory democracy, for example).

10. For online targeting to truly benefit individuals, organisations, and society, key players in the ecosystem must enhance the level of transparency, respect users' choice of how their data is collected and used, give up intrusive tracking and profiling techniques, and assume social responsibilities when developing and deploying online targeting systems.

## *2. How do organisations carry out online targeting in practice?*

### *2.1. What do organisations use online targeting for? What are the intended outcomes?*

11. Online targeting is often used for commercial advertising and political campaigning. Commercial

---

[14] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf; Frederik J. Zuiderveen Borgesius, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) 5(3) International Data Privacy Law 163.

[15] https://lumapartners.com/content/lumascapes/display-ad-tech-lumascape/

[16] For example, see http://www.aboutads.info/resource/image/Poll/Zogby_DAA_Poll.pdf. For criticisms, see http://ssrn.com/abstract=1478214.

[17] For example, see https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/ZogbyAnalyticsConsumerValueStudy2016.pdf. For criticisms, see Chris Jay Hoofnagle and Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price' (2014) 61 UCLA Law Review 606.

[18] For example, see http://www.adassoc.org.uk/wp-content/uploads/2014/09/Advertising_Pays_Report.pdf.

[19] For example, see https://www.iabuk.com/sites/default/files/The%20Data%20Deal%20-%20How%20Data%20Driven%20Digital%20Advertising%20Benefits%20UK%20Citizens.pdf.

targeting aims to identify internet users who might be interested in the advertised item, and attract them to visit the website of the advertiser (measured by click-through rate) and eventually make a purchase or sign up for the service (measured by conversion rate). Political targeting aims to identify voters or the public in general and engage or influence them in relation to an election, referendum, public vote, or the course of public discussion on a particular subject matter.

***2.2. What are the key technical aspects of online targeting? (what data is used; how is it collected, processed, and/or shared; what customisation is carried out; on what media; and how is this monitored, evaluated, and iterated on)?***

12. The technical model of a typical online targeting system involves tracking, profiling and targeting. With cookies or other online identifiers, online targeting networks can monitor an internet user's online activities across websites, services, devices and platforms. Such details will feed into the building of profiles (kept by advertisers, data brokers, intermediaries, ad network providers, and so on) drawing inferences about the user's potential interest in different advertising categories. When the user visits a different website later, the targeting system will either automatically choose an advert that fits with the user's interest profile, or initiate a real-time bidding to allow advertisers to bid for the chance to show their advert to this particular user. A wide range of data is collected, shared, circulated (especially under the real-time bidding model), linked (with cookie matching or similar techniques), and analysed. This may include their partial IP address, gender, age group, geolocation, postcode, detected language, interest categories and so on.[20]

***2.3. How is this work governed within organisations (how are risks monitored and mitigated, including unintended consequences, who is accountable within organisations, how are complaints dealt with)?***

13. No response.

***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?***

***3.1. What is the current legal and regulatory environment around online targeting in the UK? How effective is it?***

14. The regulatory measures on online targeting are primarily set out by data protection law in the UK, including the GDPR and the ePrivacy Directive, as well as their domestic implementations, namely the DPA 2018 and the PECR. The legal framework provides a set of principles and rules regarding the use of personal, which is central to the operation of an online targeting system. While there are currently legal actions across Europe against major players in the industry, such as Facebook[21] and Google[22], enforcement in the UK against unfair online targeting practices remains minimal.

15. Other areas of law, such as consumer protection law, competition law, and election law are also

[20] https://developers.google.com/authorized-buyers/rtb/downloads/realtime-bidding-proto

[21] https://www.theregister.co.uk/2018/08/01/irish_supreme_court_makes_surprise_decision_to_hear_facebooks_appeal_in_schrems_ii/

[22] https://www.theregister.co.uk/2019/02/20/iab_rtb_complain_fresh_evidence/

relevant in certain cases, and there are ongoing discussions on how cross-sector enforcement jointly by different regulators can be made possible and effective.

***3.2. How significant are the burdens placed on organisations by this environment?***

16. The industry constantly claims that they are over-burdened with compliance requirements under data protection law and may risk being outcompeted by companies from other major economies where regulation is more relaxed, such as the US and China. This is however unlikely to be the case as the extraterritorial effect of EU data protection law means that all businesses competing for the EU market are subject to the same set of data protection rules, regardless of their place of establishment.

***3.3. Are there laws and regulations designed for the "analogue" world that should be applied to online targeting in the UK?***

17. In fact, data protection law does not in principle differentiate offline and online use of personal data and applies to both contexts alike. Other areas of law in the UK, however, seem to be lagging behind in regulating online targeting. For example, competition law still largely focuses on market share and fails to capture the powerful market dominance enabled by the use of data in the online targeting sector.[23] Election law, on the other hand, while imposing strict rules on the use of funds by political parties, does not have an equally strict set of rules when it comes to the use of data for online political targeting. This would entail not just extending the scope of existing laws to cover online practices, but also sector-specific policies to restore the power dynamics disrupted by the use of online targeting.

***3.4. Are there any international examples of regulation and legislation of online targeting that we can learn from?***

18. No response.

***4. How is online targeting evolving over time, what are the likely future developments in online targeting, and do these present novel issues?***

***4.1. What emerging technologies might change the way that online targeting is carried out? Might these present novel issues?***

19. The increasingly complex statistical models of Machine Learning, often referred to as Artificial Intelligence, may be a gamechanger in the field of online targeting, as it might enable more powerful – and intrusive – targeting practices – however, these complex models are notoriously difficult to analyse in order to determine if their behaviour is discriminatory.

20. The Internet of Things (IoT) technologies may also bring about radical changes to the landscape, as the increasing popularity of IoT devices amounts not just to more channels for online targeting to exert influence, but also more data points to collect data for a fuller user profile. Importantly, such

[23] Orla Lynskey, 'Grappling with "Data Power": Normative Nudges from Data Protection and Privacy' (2019) 20 Theoretical Inquiries in Law 189.

technology may often be capturing data about people other than those who have consented, for example visitors to a house, undermining the legal basis for processing.

21. Improved tracking, profiling, and targeting techniques will also present further issues. For example, the state-of-the-art device fingerprinting technologies may allow online trackers to bypass device privacy settings and conduct invasive targeting.

***4.2. How might existing and emerging governance regimes (such as the General Data Protection Regulation, European e-Privacy and e-Commerce Directives, and potential Online Harms legislation) impact online targeting practices?***

22. As noted above, online targeting practices are already subject to existing data protection laws. However, the level of enforcement of such laws is still fairly minimal. Future legislation specifically addressing the issues of online targeting may contribute to a more fully functional regulatory environment, but the effectiveness will still depend on the performance of law enforcement.

***4.3. Are there examples of types of online targeting and personalisation (that might have either negative or positive impacts) that are currently possible but not taking place? If so, why are they not taking place?***

23. No response.