Centre for Data Ethics and Innovation: Review on online targeting

Written Submission by The Human Rights, Big Data and Technology Project

University of Essex

14 June 2019

Introduction

1. The Human Rights, Big Data and Technology Project ('HRBDT'),[1] based at the University of Essex's Human Rights Centre, welcomes the opportunity to participate in the Centre for Data Ethics and Innovation's ('CDEI') review on online targeting. Established in 2015, HRBDT identifies the opportunities and risks posed by big data and emerging technologies to human rights and proposes policy, practical and regulatory responses at the national and international level.[2] This submission addresses questions one and three of the call.

2. Online targeting (or personalisation) by companies, governments and other entities is widespread. Behavioural profiling and micro-targeting form central parts of online advertising strategies, news dissemination and products and services provision.[3] Online targeting relies on individuals' data in order to personalise products, services and information. Although it can appear relatively innocuous and convenient, online targeting raises serious human rights and data protection issues. This arises because of how data are collected, triangulated, shared and sold (including through data brokers). This can occur without the individual's consent or, where it is ostensibly given, with little awareness of how the data were obtained and what may happen to them in the future. The way in which individuals act upon products, services and informed targeted at them may also give rise to additional human rights issues.

A. Privacy and Data Protection Challenges

3. Online targeting poses threats to privacy and data protection. It raises questions on the extent to which the protections set out in the General Data Protection Regulation (GDPR) are being effectively implemented as well as whether any gaps in protection remain.

[1] The Human Rights, Big Data and Technology Project, available at <http://www.hrbdt.ac.uk>.
[2] For more information on the Project, please see Annex 1.
[3] See for example, Facebook, 'Ad Targeting'.

(1) Effectiveness of Consent Requirements in Practice

4. The first key issue relates to consent. In many instances, consent may appear to have been given, however, this may not be meaningful, raising questions of GDPR compliance. For example, consent is often secured through a pre-selected check-box, requiring active – and often complicated – opting-out.[4] Even where an 'opt-in' process is provided, in practice, individuals may not have any or sufficient information as to the purpose of the targeting, how the data will be analysed and duration of data storage. Very little transparency also exists on many websites, apps and platforms on the sharing and selling of data, despite access to and triangulation of a wide set of data about an individual being critical for targeting. Moreover, there can often be no information, particularly at the point of consent, on the risks of online targeting. Such practices may not be compliant with the requirements of the GDPR under Article 5. Moreover, the opaque and complex nature of the online targeting ecosystem may make it very difficult to achieve meaningful consent for most users, despite this being a central lawful basis under Article 6 of the GDPR[5]. Moreover, the way in which online targeting works may make it virtually impossible for an individual to assess or trace original consent or regain control over the data once it has been shared or sold. This may make the invocation of articles 15 (access to data), 16 (rectification of inaccurate data) and 17 (deletion) difficult.[6]

5. The emphasis on consent can also impose a heavy burden on users to act as their own data managers and to be aware of the risks and how to mitigate them in ways that are often cumbersome and unclear. These practices can therefore undermine individuals' free choice and their dignity and autonomy. They raise questions about how to effectively enforce the requirements of the GDPR in practice and in particular how to make consent meaningful and not a 'tick-box' exercise.

(2) Other Lawful Bases for Processing Data: Legitimate Interest

[4] Rau, Sabrina "Those pop-up 'I agree' boxes aren't just annoying – they're potentially dangerous", The Conversation, https://theconversation.com/those-pop-up-i-agree-boxes-arent-just-annoying-theyre-potentially-dangerous-106898
[5] GDPR articles on obligations of data controller and rights of individuals.
[6] David Uberti, 'Shady political ads are pouring into Facebook. We still can't track them.', Vice News, 28 May 2019, available at https://news.vice.com/en_us/article/qv7z7p/shady-political-ads-are-pouring-into-facebook-we-still-cant-track-them?utm_campaign=sharebutton.

6. Consent is not the only basis upon which targeting can be legitimized as under GDPR as it is only one of six legal bases for processing data[7], Legitimate interest is of particular concern in this regard as the legitimate interest of a commercial entity such as an advertising agency, for example, is to generate profit through its products for its shareholders. Legitimate interest in the GDPR context, however, has the caveat of only being legitimate when not in competition with fundamental rights. One challenge of not allowing targeting based on legitimate interest is to better communicate the harms of targeting.

(3) Profiling

7. Online targeting not only relies on data access and collection but also requires the building of profiles about individuals.[8] The GDPR addresses profiling in Article 4(4). However, the definition is relatively restricted. As the Article 29 Working Party demonstrates, whether the following example - which clearly links to online targeting - falls under the definition of profiling for the GDPR's purposes 'will depend on the circumstances', indicating that certain forms of profiling may not fall under the GDPR:

> A data broker collects data from different public and private sources, either on behalf of its clients or for its own purposes. The data broker compiles the data to develop profiles on the individuals and places them into segments. It sells this information to companies who wish to improve the targeting of their goods and services. The data broker carries out profiling by placing a person into a certain category according to their interests.[9]

8. All forms of profiling must comply with Article 5 and the lawful bases for data processing under Article 6 as already set out. Where a decision is made on the basis of the profiling, Article 22(1) also may apply. However, the protections of Article 22 are limited as it only provides the right to object to a decision made solely on the basis of 'automated processing' and only if it 'produces legal effects concerning him or her or similarly significantly affects him or her'. This both raises questions about the threshold for 'significant effects' in the context of online targeting and also does not cover the more common situation in which automation is part of a decision-making process.[10]

[7] Insert article on legal basis GDPR
[8] Valeria Ferraris et al., 'The Impact of Profiling on Fundamental Human Rights', PROFILING Working Paper no.3-2013, available at http://www.unicri.it/special_topics/citizen_profiling/PROFILINGproject_WS1_Fundamental_1110.pdf.
[9] Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 At 8
[10] Lorna McGregor, Daragh Murray, and Vivian Ng, "International Human Rights Law as a Framework for Algorithmic Accountability" (2019) 68(2) International & Comparative Law Quarterly, 316-318, 339-341, available in open access at <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/international-human-rights-law-as-a-framework-for-algorithmic-accountability/1D6D0A456B36BA7512A6AFF17F16E9B6>.

B. Consequences of Targeting to Human Rights

9. Beyond privacy and data protection, online targeting can produce significant harm to users, sometimes also affecting their enjoyment of basic human rights.

10. First, individuals and groups in positions of vulnerability can be particularly affected by online targeting and exposed to further abuses online. For example, studies have shown that older persons are often the preferred target for scams, phishing attacks and other fraud attempts.[11]

11. Second, there is a risk of exclusion through online targeting, meaning that since it delivers information and advertisements to what is perceived to be the most relevant audience, others, who do not fall within those parameters, may not receive the same information. Such practices can affect, for instance, the accessibility requirement of the right to work and may result in discrimination. For example, studies have suggested that online advertisements can discriminate against women, claiming that men are shown online advertisements for high-paying jobs[12] and for career coaching services for executive positions with salaries over US$200,000[13] more frequently than women. Other studies have suggested that companies that use online advertisement services are able to limit their visibility to selected age groups thus excluding older workers from seeing job advertisements.[14]

12. Third, targeting is used to provide users with news and information deemed to be the most relevant to them on the basis of their historical browsing activity and known or inferred interests, preferences, social connections and identity. This selective funneling of information operated by algorithmic content filters can create echo chambers and 'filter bubbles', whereby individuals are continuously exposed to a limited and restricted range of information. Having access to a diverse variety of information is critical for the

[11] Ben Robinson, 'Reports of frauds on the elderly are 'tip of iceberg', BBC News, 23 September 2018, available at https://www.bbc.com/news/uk-45590333.
[12] American Civil Liberties Union, 'Facebook Equal Employment Opportunity Commission Complaint', 18 September 2018 available at <https://www.aclu.org/legal-document/facebook-eeoc-complaint-charge-discrimination/>
[13] Amit Datta et al., 'Automated Experiments on Ad Privacy Settings' (2015) 1 Proceedings on Privacy Enhancing Technologies 92, 92–112
[14] Julia Angwin et al., 'Dozens of Companies Are Using Facebook to Exclude Older Workers From Job Ads' (ProPublica, 20 December 2017) available at <https://www.propublica.org/article/facebook-ads-age-discrimination-targeting>. For further discussion see also 'The Universal Declaration of Human Rights at 70: Putting Human Rights at the Heart of the Design, Development and Deployment of Artificial Intelligence', (HRBDT, 20 December 2018), available at https://hrbdt.ac.uk/the-universal-declaration-of-human-rights-at-70-putting-human-rights-at-the-heart-of-the-design-development-and-deployment-of-artificial-intelligence/.

development of opinion and thought and its lack can also ultimately diminish an individual's ability to distinguish between reliable and non-reliable information.

13. Fourth, misinformation and disinformation are also facilitated by online targeting, increasing their adverse impact on human rights. For example, so-called conspiracy theories on global warming or vaccinations and targeted attacks on human rights defenders and journalists and reporting human rights violations, are clear examples of how filter bubbles and echo chambers can serve to spread mis and disinformation.[15] Moreover, this can lead to serious threats to the health, security, liberty and life of individuals in the off-line space.

14. Misinformation and disinformation campaigns can be targeted at minorities and vulnerable groups, exacerbating societal fractures and feelings of hatred through the dissemination of selected information and messages.[16] For example, a study on the 2016 US Presidential Elections reported that African-American voters were targeted with disinformation about electoral procedures causing their votes to be invalidated.[17]

15. Finally, as confirmed by recent data from the Office for National Statistics, although the number of people with access to internet is increasing, there is still an average of 20% without basic digital skills.[18] For them, the online space is complex and difficult to access and social media platforms are often the first and only point of entry. They can be particularly susceptible to online targeting and misinformation and disinformation campaigns. Such a situation, besides affecting their right to receive information, freedom of thought and opinion, may also increase and amplify existing discrimination.

Conclusion and Recommendations for Addressing the Potential Harm Caused by Online Targeting

16. As set out above, the first critical action that is required is an assessment of how to ensure that the requirements of the GDPR are being effectively implemented and not circumvented by opaque, time-

[15] See, for instance, Carly Nyst and Nick Monaco, 'State-sponsored trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns' (Institute for the Future & Digital Intelligence-Futures Lab, 2018), available at http://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf and Claire Wardle & Hossein Derakhshan, 'Information Disorder. Toward an interdisciplinary framework for research and policymaking' (Council of Europe Report DGI 09-2017, 27 September 2017).
[16] Renee Di Resta et al., 'The Tactics & Tropes of the Internet Research Agency' New Knowledge Report, December 2018, available at https://cdn2.hubspot.net/hubfs/4326998/ira-report-rebrand_FinalJ14.pdf
[17] Philip N. Howard et al. 'The IRA, Social Media and Political Polarization in the United States, 201-2018' (Working Paper 2018.2, Oxford Project on Computational Propaganda).
[18] Office for National Statistics, Exploring the UK's digital divide, 4 March 2019, available at https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/articles/exploringtheuksdigitaldivide/2019-03-04#why-does-digital-exclusion-matter.

consuming and complex consent processes or a lack of adequate information. HRBDT recommends that a clear articulation of how the GDPR applies to online targeting is produced. This should set out the measures actors engaged in profiling are required to take in relation to issues such as clear and usable consent processes; processes for individuals to trace, obtain and delete data; and clarity and notification on the collection, analysis, sharing and sale of data. It should also include clear processes whereby not only companies but also states are transparent in their own use of targeting as well as how they benefit from data, profiling and insights developed by others through online targeting.

17. A gap-analysis also needs to be undertaken into any issues remaining, particularly in relation to profiling. Such an analysis should be informed by international and national human rights law in addition to data protection law in order to ensure that the full extent of the potential harm posed by online targeting is addressed and that practical measures, such as impact assessments, are not constrained to privacy or data protection alone. Embedding human rights within responses to online targeting, also places the individual at the centre, empowering individuals to claim their rights and imposing specific human rights obligations on the duty-bearers.

18. Given the global nature of the internet as well as major technology companies, the most effective solutions to online targeting will be developed multilaterally and through multi-stakeholder initiative, as has already been demonstrated by through the GDPR and other key work undertaken by the European Union in this space. The UK should therefore both analyse how it can more effectively address the risks of online targeting through its national law and policy and at the regional and international level.

19. It is critical, however, that any response to the risks posed by online targeting, particularly with regard to mis and disinformation, does not result in overly restrictive laws that adversely affect human rights or the actions of parts of a democratic society, such as civil society, as has been witnessed in a number of states through the development of ‘fake news’ laws.

20. In addition, more attention should be dedicated to education, ensuring media and digital literacy are made part of the national curriculum. This will enable individuals to protect themselves against the malicious use of online targeting, especially in situations such as misinformation and disinformation.

Annex 1

About the Human Rights, Big Data and Technology Project

1. The Human Rights, Big Data and Technology Project (HRBDT) began in 2015 with £5 million funding from the Economic and Social Research Council and further funding from the University of Essex. One of the largest of its kind in the world, the Project is based at the Human Rights Centre at the University of Essex with over 30 academics, and additional researchers based at Cambridge University, the Geneva Academy and Queen Mary University. The team addresses human rights and technology issues across a range of disciplines including computer science, economics, law, philosophy, political science, communication studies and sociology.

2. The core objective of HRBDT is to identify and assess the risks and opportunities for human rights posed by big data, artificial intelligence and smart technologies and to propose solutions to ensure that new and emerging technologies are designed, deployed and regulated in a way that is enabling of, rather than threatening to, human rights. HRBDT's research assesses the adequacy of existing ethical and regulatory approaches to big data and new and emerging technologies from a human rights perspective. HRBDT's research also demonstrates how human rights standards are capable of adapting, and offering solutions to, rapidly evolving technological landscapes. We engage with responses to the risks and opportunities posed by data and technology at the multilateral and multi-stakeholder level as well as within specific sectors, such as the law enforcement, health, education, social care, and humanitarian sector, and at the national level in States such as Brazil, Germany, India, the UK and the US.

3. Our cutting-edge research focuses on engagement with and informing the practices of transnational governance (particularly at the UN level) and across multiple national level bodies in States such as the Brazil, Germany, India, the UK and the US. Focused on producing evidence-based and innovative research to support decision-making in policy, regulatory and commercial settings, HRBDT has been at the forefront of national and international debates on the human rights impact and governance of big data, artificial intelligence and a range of emergent technologies since its inception. Our research provides greater insight into the range of opportunities and risks relating to the use of AI, and guidance as to how AI can be developed and deployed in a human rights compliant manner.

4. For example, HRBDT is regularly invited to speak on panels at the UN Human Rights Council, at expert meetings at organised by the Office for the High Commissioner for Human Rights and the Office for the High Commissioner for Refugees, and high-level multi-stakeholder global forums such as the AI for Good Global Summit organised by the International Telecommunication Union and the UN Internet Governance Forum. HRBDT engages with businesses such as British Telecom and Microsoft on the human rights impact of data and AI and possible responses. HRBDT also frequently engages with national bodies, agencies and organisations including the Investigatory Powers Commissioners Office, the Home Office, a range of law enforcement bodies, a number of Select Committees, and the Law Society. HRBDT works in partnership with a range of civil society organisations in the UK and overseas including the American Civil Liberties Union, Amnesty International and Liberty.

5. Working with both national and international actors, HRBDT is strategically positioned with insight on how State and business practice at the national level feeds into contemporary debates, as well as how the international human rights legal framework is translated and implemented domestically. This dual-focus through the lens of the UN space enables a two-way flow of ideas and approaches, which is of significant benefit to governance debates.

Professor Lorna McGregor
Dr Elena Abrusci
Sam Dubberley
Sabrina Rau
Human Rights, Big Data and Technology Project