PRIVACY INTERNATIONAL

Submission to the Centre for Data Ethics and Innovation's review of online targeting

June 2019

Privacy International submission to the Centre for Data Ethics and Innovation's Review of Online Targeting

14 June 2019
By email: policy@cdei.gov.uk

Privacy International (PI) welcomes the opportunity to respond to this consultation. Established in 1990, PI is a non-profit organisation based in London, dedicated to defending the right to privacy around the world.

In considering the impact of online targeting, it is essential that the Centre for Data Ethics and Innovation have due regard for privacy as a fundamental right (as enshrined in UK, European, and International Law). Privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. For people to fully participate in democratic society, developments in law and technologies must strengthen and not undermine peoples' ability to freely enjoy these rights.

PI is responding to the call for evidence for the online targeting review.

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

Over the past decade online targeting has become much more invasive. Targeting today, specifically online targeted advertising, is enabled by the collection, sharing, and processing of massive amounts of people's data. People are often unable to meaningfully understand how their data is collected, shared, and used.

Online targeted advertisement is facilitated by a complex and opaque ecosystem that includes AdTech companies and other third-parties[1]. Reports from the UK's Information Commissioner Office (ICO)[2] highlight concerns with the use of personal data for targeted advertising[3][4].

Online targeting has become virtually inescapable and the ecosystem is so complex that it has become impossible for people to know where their data ends up and how they are being targeted.

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

---

[1] See: https://privacyinternational.org/long-read/2967/ad-supported-internet-broken-inefficient-and-privacy-nightmare-lets-fix-it
[2] See: https://ico.org.uk/media/action-wevetaken/2259369/democracy-disrupted-110718.pdf
[3] See: https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analyticsfor-political-purposes-update.pdf
[4] See: https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

1.1.1. Its impact on our autonomy

When considering the impact of online targeted advertisement on the autonomy, it is important to examine the issue through the lens of data in politics. While this is not the only lens by which to consider the impact of autonomy, it is what our response will focus on.

Democratic elections are complex processes and their functioning demands the collection and processing of personal data. Personal data increasingly plays a fundamental role in the emerging way of influencing democratic processes. Through the amassing and processing of vast amounts of data, individuals are profiled[5] based on their stated or inferred political views, preferences, and characteristics. These profiles are then used[6] to target individuals with news, disinformation, political messages, and many other forms of content aimed at influencing and potentially manipulating their views. It is extremely difficult, if not impossible[7], to opt-out of all the existing tracking methods.

1.1.2. Its impact on vulnerable or potentially vulnerable people

The complex and opaque ecosystem of data exploitation that facilitates online targeted advertisement demands the collection and sharing of people's personal data with innumerable third parties.

The harms and risks of such data sharing can be exacerbated when experienced by those in vulnerable situations. The collection of sensitive data – even if not overtly sensitive – can result in targeting that can reveal very personal information and serve to exacerbate[8] existing inequalities.

Further, targeted ads can be discriminatory[9] (a person might not be not shown a job[10] because they are a woman or a loan because they live in the wrong neighbourhood[11]), they can seek to be manipulative[12] (a person is served tailored information to target those that are most vulnerable), and a user may have no control[13] over how this data is shared[14] and repurposed (say, with data brokers and others who are selling personal information to people outside the advertising ecosystem, including political actors).

---

[5] See : https://privacyinternational.org/feature/1721/snapshot-corporate-profiling
[6] See: https://ico.org.uk/media/action-wevetaken/2259369/democracy-disrupted-110718.pdf
[7] See: https://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found
[8] See: https://privacyinternational.org/case-studies/737/case-study-invisible-discrimination-and-poverty
[9] See: https://dataprivacylab.org/projects/onlineads/1071-1.pdf
[10] See: https://www.bbc.co.uk/news/technology-45569227
[11] See: https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html
[12] See: https://privacyinternational.org/long-read/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack
[13] See: https://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found
[14] See: https://rewire.news/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/

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

The collection, processing, and sharing of data that underpins online targeting together with its use to infer, derive, and predict more data about people (profiling) raises serious concerns for the right to privacy and data protection.

Many companies that are part of the ecosystem underpinning online targeting fail to meet the requirements of data protection law. PI have complained about seven such companies to Data Protection Authorities in the UK, Ireland, and France[15]. Our complaints describe why the use of the data for online targeting fails to meet the requirements of many of the data protection principles.

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)?

Platforms and third-party companies track[16] users on websites, smartphones, and increasingly also on smart devices. Platforms have the advantage that they are present in many of these places already which allows them to learn[17] about user behaviour on millions of websites and apps.

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?

Data Protection Law

Data protection law in the UK (the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 ("DPA")) strengthens the rights of individuals with regard to the protection of their data, imposes more stringent obligations on those processing personal data, and provides for stronger regulatory enforcement powers – in theory.

The law requires that the processing of personal data (including profiling) complies with the following principles: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality.

---

[15] See: https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad

[16] See: https://privacyinternational.org/explainer/2976/how-do-tracking-companies-know-what-you-did-last-summer

[17] See: https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf

Among other obligations, data controllers must have a lawful basis for processing personal data (in online advertising this is often claimed to be consent or legitimate interest) and to facilitate individual's exercise of their rights (such as the right to information, the right to access data, an absolute right to object to direct marketing and the right to erasure).

Furthermore, there are prohibitions on certain types of processing, including in relation to personal data revealing special category data (such as racial or ethnic origin, political opinion, religious or philosophical beliefs, health, sex life or sexual orientation) – without explicit consent – and also in relation to automated decisions, including profiling, which produce legal or other significant effects.

That targeted advertising can have significant effects on people is acknowledged[18] in the Article 29 Working Party Guidelines (adopted by the European Data Protection Board) on Automated individual decision-making and Profiling, however, as far as PI are aware, there are no specific decisions dealing with this question yet.

In practice, the real test for the online targeting ecosystem will be enforcement, as to-date there has been wide scale disregard of the law – as highlighted in PI's complaints[19] on this issue. Enforcement must be accompanied and followed by proactive implementation by companies.

PI responded to the ICO's consultation on a Code of Practice on the use of personal data in political campaigns[20], another area in which further guidance and enforcement are needed.

Furthermore, there remain outstanding issues with the implementation of derogations in the GDPR in the UK through the DPA which impact on the law's effectiveness in relation to online targeting. These issues were highlighted by PI[21] during the passage of the legislation.

ePrivacy

In the UK, the Privacy and Electronic Communication Regulations (PECR), implement the European Directive 2002/58/EC "the ePrivacy Directive". This governs confidentiality of communications which includes storing information in or gaining access to information stored in the "terminal equipment" (e.g. computer, smart phone) of a subscriber or user. This is the so called "Cookie law", which requires that subject to certain exceptions, users must be provided with clear and comprehensive information and provide their consent before such tracking.

---

[18] See: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwi9uaK2vObiAhX76OAKHbguDygQFjAAegQIBBAC&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fdocument.cfm%3Fdoc_id%3D49826&usg=AOvVaw3Hbd9vdV-5JxpwJPUmrucm

[19] See: https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad

[20] See: https://privacyinternational.org/advocacy/2838/pi-response-ico-call-views-code-practice-use-personal-information-political-campaigns

[21] See: https://privacyinternational.org/sites/default/files/2018-05/Privacy%20International%20Amendments%20DPB%20post%20Committee%2018-04-2018.pdf

There are other frameworks and regulators that are also important to look at, including Equality Law, Consumer Protection, and the Advertising Standards Authority. Due to the word count limitation we have not commented on the effectiveness of these regimes and have focused on the UK's Data Protection Act.

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

Focussing particularly on the issue of targeted advertising in the political context, we encourage the CDE to review the recommendations made by the Electoral Commission around digital campaigns[22].

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

As highlighted elsewhere in our submission, the key framework at this time worldwide for regulating the use of data for targeting, is data protection law. As well as the ICO, other DPAs are looking at this issue, including in Ireland and France[23].

There are also emerging transparency efforts, particularly in relation to political advertising, for example the Elections Modernization Act (Bill C-76)[24] in Canada which requires the creation of political advertisement registries. In the US, a proposal for an Honest Ads Act[25] was introduced, and in Ireland the Private Member's Bill, Online Advertising and Social Media (Transparency) Bill 2017[26] was produced, although it is unlikely to progress further.

The EU has also sought commitments from platforms as to ads transparency[27]. Electoral advertising will also tend to be regulated by national electoral laws, and political speech is entitled to certain protections.

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

[22] See: https://www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf
[23] See: https://www.iabeurope.eu/policy/the-cnils-vectaury-decision-and-the-iab-europe-transparency-consent-framework/
[24] See: http://www.parl.ca/DocumentViewer/en/42-1/bill/C-76/royal-assent
[25] See: https://www.congress.gov/bill/115th-congress/senate-bill/1989
[26] See: https://www.oireachtas.ie/en/bills/bill/2017/150/?tab=bill-text
[27] See: https://privacyinternational.org/news-analysis/2824/european-parliament-elections-protecting-our-data-protect-us-against

There have been radical changes to advertising over the past few years – the increased wealth of data[28] that is available for targeting, how this data can be linked[29], how many further insights can be derived from this data[30], and where people can be targeted. Websites, apps, smart devices now all contain a variety of unique identifiers[31] that allow peoples' patterns to be tracked and exploited by advertisers, including by political actors.

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?

The European e-privacy regulation is needed to protect privacy and security of data in our devices, in transit across communications networks, and at rest in companies' servers. It complements and specifies the rules of GDPR and updates the current e-privacy directive.

Since GDPR took effect, the definition and conditions of consent under ePrivacy are now equivalent to GDPR, meaning that consent has to be informed, explicit, unambiguous, and specific. However, this framework is in urgent need of revision. The proposed ePrivacy Regulation should be taken forward for this purpose.

We have outlined the role of GDPR above and plan to respond separately to the Online Harms white paper consultation.

Generally, PI would warn against knee jerk regulation – which can be broad in scope but vague in substance. For example, Singapore is aiming to regulate against the amorphous concept of 'fake news' through the Protection from Online Falsehoods and Manipulation Bull which would make it illegal to spread "false statements of fact" and would punish people with huge fines and long jail terms[32].

[28] See: https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data
[29] See: https://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found
[30] See: https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad
[31] See: https://privacyinternational.org/explainer/2976/how-do-tracking-companies-know-what-you-did-last-summer
[32] See: https://www.poynter.org/ifcn/anti-misinformation-actions/

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471