PRIVACY INTERNATIONAL

Submission to the All-Party Parliamentary Group on Electoral Campaigning Transparency

July 2019

About Privacy International

Privacy International (PI) is a leading charity advocating for strong national, regional, and international laws that protect the right to privacy around the world. Founded in 1990 and based in London, PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks.

PI employs technologists, investigators, policy experts, and lawyers, who work together to understand the technical underpinnings of emerging technology and to consider how existing legal definitions and frameworks map onto such technology.

PI is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Parliament of the United Kingdom, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

From your/your organisation's perspective, WHAT are the top issues we should be aware of with regard to each of the below: Transparency; deterrence; monitoring

Transparency and monitoring

Privacy International believes that transparency of digital advertising and online political campaigning is fundamental to ensure free and fair elections in the modern age. Political campaigns around the world have turned into sophisticated data operations. The Cambridge Analytica scandal, while not unique, raised awareness about the potential impact of the combination of profiling, micro-targeting and powerful machine learning on electoral processes.

Privacy International has documented how online targeted advertising is facilitated by a complex and opaque ecosystem that includes AdTech companies, data brokers, and other third-party companies that track people on websites and apps and combine this data with offline information. Profiling and data-driven targeting techniques used by the broader digital advertising industry are increasingly deployed in the political campaigning context, with various companies offering specific services tailored to the election context. In the UK, the Information Commissioner's report Democracy Disrupted[1] and updates to the DCMS Committee in July[2] and November[3] 2018 reference a number of such companies.

Companies and political parties are subject to the principle of transparency under Article 5 of GDPR and under a duty to provide information to those whose data they process (Article 13 and 14 of GDPR) as well as information as how it has been processed and to provide access to it (Article 15 of GDPR). To date, there is a long way to go in terms of their compliance with these provisions (as Privacy International highlighted in submissions[4] to the ICO and other data protection authorities about a number of companies in the data broker and ad tech sector). GDPR is only just over a year old and still in the early phases of enforcement. More needs to be done to ensure that all actors pro-actively implement and respect these obligations.

Transparency at every level must be proactive and up to date. Adequate information should be provided to voters explaining why they are receiving a particular message, who is responsible for it, and how they can exercise their rights to protect their data and prevent being targeted. Such transparency should not be limited to advertising, but also include the delivery of other content, such as the methods of curation, filtering, pushing, and recommendation of content.

Transparency to individuals about why they are seeing a particular message must be accompanied by transparency by political parties and campaigns of the tools and services they are using, as well as their messaging. This includes providing much more information on the sources of data, what is being done with that data, who is being targeted with what messages and what companies are being contracted and for what services, such as a campaign software, consultancy services etc.

---

[1] https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

[2] https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf

[3] https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

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

Political parties and other political actors should, as a minimum:

- ensure that the public can easily recognise political messages and communications as well as the party, foundation or organisation behind them. They should make available on their websites and as part of the communication, information on any targeting criteria used in the dissemination of such communications.
- be transparent as to the third parties they contract with as part of their campaigns both to obtain data and to further process data, including profiling and targeting, such as data brokers and political advertising companies together with those that provide consultancy services and software.

Companies that are hosting or distributing political advertising must, at a minimum, disclose information as to:

- how political advertising and social 'issue-based' advertising is defined;
- number of impressions that an ad received within specific geographic and demographic criteria (e.g. within a political district, in a certain age range), broken down by paid vs. organic reach;
- targeting criteria used by advertisers to design their ad campaign, as well as information about the audience that the ad *actually* reached;
- information about ad spend per political actor;
- information about microtargeting, including whether the ad was a/b tested and the different versions of the ad; if the ad used a lookalike audience; the features (race/ ethnicity, gender, geography, etc.) used to create that audience; if the ad was directed at platform-defined user segments or interests, and the segments or interests used; or if the ad was targeted based on a user list the advertiser already possessed.

Recently, a variety of transparency tools have been developed, including extensions which users can add, such as WhoTargetsMe[5] or recently in Argentina Publi Electoral[6] , and ad archives by major platforms. These responses are important in terms of the information that is provided to individuals and also the information that can be gathered for the purposes of research and scrutiny. The ad archives are a work in progress and there remains much to be done. It is still unclear how they apply across the world and researchers have faced difficulties[7] despite setting out some steps that could be taken to make the ad archives more effective.[8]

Furthermore, despite political parties and campaigns being required to provide certain information as noted above, privacy policies where at least some level of transparency could be provided without reliance on third parties, also to do not provide enough details. For example, see our analysis of the Conservative party leadership campaign.[9] Further transparency was also a key part of the EU Code of Practice on Disinformation.[10]

---

[5] https://whotargets.me/en/

[6] https://publielectoral.adc.org.ar/

[7] https://blog.mozilla.org/blog/2019/04/29/facebooks-ad-archive-api-is-inadequate/

[8] https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/

[9] https://privacyinternational.org/long-read/3019/how-uk-conservative-leadership-race-latest-example-political-data-exploitation

[10] https://privacyinternational.org/news-analysis/2824/european-parliament-elections-protecting-our-data-protect-us-against

Privacy International recommends that the APPG map out such tools and efforts, in consultation with those regulators already considering this issue, including the UK ICO and the Electoral Commission as well as civil society and researchers.

Deterrence

The GDPR and the Data Protection Act 2018 ("DPA") already provide the UK with tools to begin to tackle some of the issues of concern to the APPG. Privacy International encourages measures to support the enforcement of this regulatory regime. In theory, data protection law in the UK 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 practice, just over one year on, a lot more still needs to be done and changes are only starting to take place.

Privacy International has identified three main shortcomings related to the deterrence/enforcement legal framework in the UK.

First, the DPA contains exemptions for political parties that threaten to undermine protections. Paragraph 22 of Schedule 1 of the DPA 2018 permits political parties to process personal data "revealing political opinions" without the need for consent.

Privacy International and other organisations expressed serious concerns about this loophole during the drafting the DPA 2018, and we called (so far to no avail) on all main UK political parties to publicly commit not using the exemption provided in the law to target voters - both online and offline - in all local and national forthcoming elections or by-elections.[11] A similar provision in the Spanish data protection law has since been declared unconstitutional[12] and another in Romania is the subject of a complaint to the European Commission.[13]

PI recommends that the APPG investigate how and for what purposes political parties in the UK are relying on this provision.

Second, there is a need for collective redress mechanisms that empower civil society, which are currently not envisioned in the law.

Regulatory regimes are stronger and more effective if the ability of individuals to make complaints is supplemented by the ability of civil society acting in the public interest to bring complaints. This is particularly important if complaints are to address and prompt scrutiny of systemic issues, including those that might impact on more than one individual, particular groups, or society as a whole. This is recognised to an extent, for example, in the introduction of Police Super-complaints.[14] This mechanism has been used by Liberty and Southhall Black Sisters to challenge Police data sharing for immigration purposes.[15]
Such mechanisms are particularly important from a privacy perspective, as privacy invasions are often invisible, harms frequently only happen in the future, and they always affect some

[11] https://privacyinternational.org/press-release/2032/privacy-international-asks-major-uk-political-parties-commit-not-using-legal

[12] https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/Press%20Release%20No.%2076.2019.pdf

[13] https://privacyinternational.org/news/2735/romanian-ngo-files-complaint-european-commission-national-implementation-gdpr

[14] https://www.gov.uk/government/collections/police-super-complaints

[15] https://www.gov.uk/government/publications/police-data-sharing-for-immigration-purposes-a-super-complaint

people more than others. The need for a form of collective redress and to empower civil society to take action is recognised in Article 80(2) of GDPR. Article 80(2) provides for the ability of "not-for-profit body, organisation or association, which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data" to make complaints and seek an effective remedy under GDPR independently of a data subject's mandate. The benefits of such a provision have been explained by the European Data Protection Supervisor[16] and by Privacy International.[17] In spite of this, Article 80(2) of GDPR was not implemented in the DPA. Instead, it will be the subject of a review 30 months from the DPA having come into force (section 189(2)(c) of the DPA).

PI encourages the APPG to consider mechanisms for the introduction of a super complaints or other forms of collective redress (such as in Article 80(2) of GDPR) to enable civil society to tackle systemic issues undermining protections for individuals and society. Any such measure should supplement and bolster, not replace, the ability of individuals to complain and/or to be represented by civil society in complaints. At a minimum, the APPG should engage with the promised review of Article 80(2).

Third, there is a need for joint cooperation and enforcement between regulators.

Threats to the election come from different actors and require both the engagement of multiple regulators as well as coordination among them. This need for coordination in enforcement (and monitoring) was highlighted in measures adopted by the EU in the run up to the 2019 European Parliament elections. The EU demanded measures from European member states, particularly focussing on cooperation between national authorities with competences in electoral matters and authorities in connected fields (such as data protection authorities, media regulators, cyber security authorities etc).

Given the role of personal data, it was considered of particular importance that the data protection authorities collaborate with relevant election authorities both at national and European levels, including in sanctioning infringement of data protection rules where such infringement is linked to political activities by a political party[18] As noted by the European Commission, "it should be possible to impose sanctions on political parties or political foundations that take advantage of infringements of data protection rules with a view to deliberately influencing the outcome of elections to the European Parliament."

For that purpose, a procedure at the European level has been introduced to ensure the sanctioning of actions that not only breach people's privacy but that "could also potentially influence the outcome of elections to the European Parliament". The proposal allows for the sanctions to be imposed by the Authority for European Political Parties and European Political Foundations. They could amount to 5% of the annual budget of the European party or foundation concerned. In addition, the European party or foundation subject to a sanction would not be able to receive funding from the EU budget the following year.

[16] https://edps.europa.eu/press-publications/press-news/blog/civil-society-organisations-natural-allies-data-protection_en

[17] https://privacyinternational.org/blog/1050/why-we-need-collective-redress-data-protection

[18] https://privacyinternational.org/news-analysis/2824/european-parliament-elections-protecting-our-data-protect-us-against

PI recommends the APPG consider mechanisms to ensure stronger cooperation among regulatory authorities in this field as well as engagement with other regulators and legislatures looking at similar issues around the world.

From your/your organisation's perspective, HOW would you propose dealing with the top issues you raised in each area? Laws, regulations and specific recommendations are appreciated: Transparency; deterrence; monitoring

Our proposals are incorporated into our previous answer addressing the top issues.

If not previously addressed, do you have specific thoughts on the below four proposals?

(1) Provide the Electoral Commission with the resources they need to promptly investigate and prosecute those who break electoral law with specialised electoral offence officers. Fines for electoral offences should be unlimited rather than a maximum of £20,000, which is an insufficient deterrent.

If we look at this issue form a data protection perspective, we can see that a lack of or weak enforcement also creates a culture of non-compliance. The previous maximum fine of £500,000 under the Data Protection Act 1998 did not appear to act as a significant deterrent, as many of the practices which we see today would have fallen short of the DPA 1998's requirements. For this reason, Data Protection Authorities were further empowered under GDPR to fine up to, the greater of €20millon or 4% of global annual turnover. The Electoral Commission could no doubt benefit from being similarly empowered. However, monetary penalties should not be the only sanction and consideration should be given of what type of behaviour can be prohibited as part of a sanction.

(2) Report campaign spending online. Even candidate campaigns should be required to declare their expenditures online. This includes creating a national database for election spending.

Privacy International supports the proposal to include additional requirements related to expenditures for online campaigning. Political parties and other actors are increasingly using social media platforms and other digital communications means both for targeting potential individual donors (particularly for small donations) and for spending on political advertising.

Campaign financing is notoriously difficult to monitor. Even more, recent and ongoing investigations have shown how the traditional rules of campaign financing fail to regulate and shed a light on these new forms of online fundraising and expenditures. In its 2018 report on online manipulation and personal data, the European Data Protection Supervisor noted that "the reported spending on campaign materials may not provide sufficient details about spending on digital advertising and associated services, e.g. targeted ads on social media, analytics services, creation of voter databases, engagement with data brokers.".[19] In this regard we note that the Electoral Commission has also called for changes in the laws to increase transparency for voters in digital campaigning, including on spend.[20]

[19] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[20] https://www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf

Privacy International recommends that campaign finance law require timely online reporting on spending on online campaigning and on the funding obtained online. The information should be sufficiently granular and detailed to promote transparency and accountability. This should include provisions to require political parties and other political actors to make publicly available (e.g.as a minimum, prominently on their websites) information on their expenditure for online activities, including paid online political advertisements and communications. This should include information regarding which third parties, if any, have assisted the political actors with their online activities, including the amount spent on each third parties' services.

To ensure effective monitoring the disclosure of campaign expenditure should be broken down into meaningful categories such as amount spent on types of content on each social media platform, information about the campaign's intended target audience on platforms, as well as actual reached audience. Additionally, the law should require the disclosure of information on groups that support political campaigns, yet are not officially associated with the campaign, and disclosure of campaign expenditure for online activities, including paid online political advertisements and communications.

(4) Ensure parity between political offline and digital advertising in the election period. This includes creating an online repository of all digital ads, enforcing imprints on digital ads and making targeting and financing details less than two clicks away.

One of the current key campaigning safeguards is to ensure that political parties and other contestants have equal and fair access to traditional media and that reporting by publicly owned media is fair and not partisan. The rationale for these obligations (of impartiality, fairness, balance, and equality during elections) is the 'scarcity assumption', i.e. the fact that opportunities to access traditional media are limited. This 'scarcity', it is assumed, would not apply to online media, given the facility and variety of sources of opinions and access to them. However, this assumption does not take into consideration the market concentration in the digital communications field and the way information is distributed and shared by digital platforms (notably search engines and social media platforms, including messaging apps).

A few giant tech companies act as gatekeepers of the digital content which most individuals access online. As noted by the European Data Protection Supervisor, "data analytics could help individuals navigate through the increasingly noisy information environment" but "in effect, the forum for public discourse and the available space for freedom of speech is now bounded by the profit motives of powerful private companies.[21]

In particular, search engines and social media platforms filter the news and opinions users access based on profiling. This goes beyond paid-for targeted advertisements and promotion of content to the way all content is displayed and recommended (for example, the personalisation of Google search results[22]; Facebook's newsfeed[23]; or YouTube's recommendations.[24] These data targeting techniques expose individuals only to selected political messages and political information, directly challenging the assumption that a wide spectrum of opinions and content in the online media is easily available to anyone. Effects like filter bubbles, etc. are direct consequences of such targeting and have significant effects on the formation of political opinions and ultimately on elections.

[21] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[22] https://www.google.com/search/howsearchworks/algorithms/
[23] https://www.facebook.com/help/1155510281178725
[24] https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html

Privacy International acknowledges that regulating the online space is complex and fraught with risks (including of unduly limiting freedom of expression and of access to information) For these reasons, Privacy International advocates for caution. However, there are some measures, based on existing obligations under data protection law, that require urgent enforcement and would provide some protection. At the very minimum, internet and social media platforms must be transparent about their profiling activities, including for the personalisation of what people see. The use of personal data for profiling must also comply with data protection standards.

Additionally, Privacy International supports the adoption of measures aimed at enhancing transparency in this field (as noted in the previous answer.) Given the difficulties in defining what constitutes political advertising and the many actors involved, effective ads transparency must go beyond just political ads or scrutiny limited to one particular platform. Solutions must enable meaningful transparency for users as well as enable effective scrutiny by researchers and civil society.

The APPG should consider how these challenges might be surmounted, for example with an online repository of all digital ads.

Is there anything else you would like to share with the APPG?

Privacy International has recently published a few briefings related to data and elections which may be of interest to the APPG, including:

- Data Exploitation and Democratic Societies: https://privacyinternational.org/long-read/2850/data-exploitation-and-democratic-societies
- Technology, data and elections: A 'checklist' on the election cycle, June 2019: https://privacyinternational.org/advocacy/3093/technology-data-and-elections-checklist-election-cycle
- European Parliament elections – protecting our data to protect us against manipulation (https://privacyinternational.org/news-analysis/2824/european-parliament-elections-protecting-our-data-protect-us-against)
- Privacy International's Response to the Open Consultation on the Online Harms White Paper: https://privacyinternational.org/sites/default/files/2019-07/Online%20Harms%20Response%20-%20Privacy%20International_0.pdf
- When your data becomes political, video: https://privacyinternational.org/video/2937/video-your-vote-sale-political-advertisers-think-so
- Privacy International's Response to the ICO's Call for Views on a Code of Practice for the use of personal information in political campaigns : https://www.privacyinternational.org/advocacy/2838/pi-response-ico-call-views-code-practice-use-personal-information-political-campaigns

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