Submission to the UK Committee on Standards in Public Life on electoral campaigning

July 2020

privacyinternational.org

Submission to the Committee on Standards in Public Life

About Privacy International

Privacy International (PI) is a leading UK registered 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.

Q1 What values do you think should underpin the regulation of donations and loans, and campaign expenditure by candidates, political parties and non-party campaigners in the UK, and why? Such values may include, though are not limited to, concepts such as transparency, fairness and accountability.

Transparency

Transparency is key in the political campaigning environment. Though an established principle of public life, the articulation of transparency or openness in the Nolan Principles does not sufficiently address the reality of elections in the modern age.

Political campaigns around the world and in the UK have turned into sophisticated data operations. As revealed by the Cambridge Analytica scandal, 'invisible' or 'hidden' mechanisms in online political advertising have a growing impact on electoral processes and outcomes. Through profiling, micro-targeting, and powerful machine learning, potential voters can be targeted with finely-honed messages tailored to their interests, views, or personality traits. Digital advertising accounted for 42.8% of campaign spending in the UK in 2017[1] – the most recent year for which data exists – yet very little is known about the systems behind political ads.

Privacy International has documented how online targeted advertising is facilitated by a complex and opaque ecosystem that includes AdTech companies[2], data brokers[3], and other third-party companies that track people on websites and apps and combine this data with other online and offline information. Profiling and data-driven targeting techniques[4] used by the broader digital advertising industry are increasingly deployed in the political campaigning environment, with various companies offering specific services tailored to the election context. In the UK, the Information Commissioner's report *Democracy Disrupted?*[5] and updates to the DCMS Committee in July[6] and November[7] 2018 reference a number of such companies. The current lack of transparency by political campaigns and those companies they work with is a significant obstacle to scrutinising their practices, further eroding trust in the campaigning environment and the electoral process.

It is unclear from where political parties and the companies they employ to run digital political campaigns are getting their data. In October 2019, PI was one of six organisations which jointly wrote to all the political parties in the UK to ask

---

[1] https://www.electoralcommission.org.uk/cy/node/534
[2] https://privacyinternational.org/learn/adtech
[3] https://privacyinternational.org/advocacy/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and-what
[4] https://privacyinternational.org/news-analysis/3735/why-were-concerned-about-profiling-and-micro-targeting-elections
[5] https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf
[6] https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf
[7] https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics- in-political-campaigns-final-20181105.pdf

which companies they were working with and where they got data from. We were very concerned that we received little to no response.[8]

Privacy International believes that the obligation of transparency should not merely be applied to the Electoral Commission as a public body, but should extend to those regulated by the Electoral Commission and relevant third parties in the interest of free and fair elections, and in line with the transparency obligations imposed by the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Companies and political parties are subject, among others, to the principles of transparency and accountability, as enshrined in the GDPR, and moreover need to abide by several obligations, such as those that oblige them to provide information to individuals (data subjects) with regard to their data practices (Article 13 and 14 of GDPR). Data protection laws also oblige them to facilitate the effective exercise of individuals' data protection rights, such as their right to access their data, their right to have their data deleted, or the right to restrict the processing. To date, there is a long way to go in terms of their compliance with these provisions, as Privacy International highlighted in submissions to the ICO[9]. To the extent that political parties are answerable to the Electoral Commission, the latter is uniquely placed to improve transparency standards. The Electoral Commission should hold all actors in the electoral ecosystem, and in particular political parties, and platforms facilitating online campaigning, to high transparency standards in its monitoring activities. Privacy International makes more detailed suggestions with regard to the nature of such transparency in relation to the financial aspects of digital campaigning in response to Q3.

Fairness

Free and fair elections are not only the linchpin of democracy, but an obligation under international law.[10] However, elections can hardly be said to be fair in an age where online campaigning is rampant and consequential,[11] and voters resent the data-driven mechanisms used therein. Only this year, in a poll carried out by Privacy International and Open Rights Group, half of respondents opposed the use of targeted ads during elections.[12]

Data protection principles provide a yardstick by which fairness in elections can be measured. But the way in which data is increasingly used in digital campaigning can hardly be said to be fair in circumstances where individuals to

[8] https://privacyinternational.org/sites/default/files/2019-10/Letter-to-Political-Parties.pdf
[9] https://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad
[10] Article 21 of the Universal Declaration of Human Rights (UDHR); Article 25 of the International Covenant on Civil and Political Rights (ICCPR); Article 3 of the First Protocol to the European Convention on Human Rights (ECHR).
[11] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[12] https://privacyinternational.org/video/3956/public-opinion-about-data-driven-election-campaigning-uk

whom that data pertains are unaware of the full extent of its use, and many of those who are aware of it find it unacceptable.

Voters should know how their data is being used at every stage of political campaigning. From collection - what data is being gathered about voters (e.g. whether they've voted before, their phone number, email or online identifiers), from where (e.g. voter lists, data brokers or social media), to how voters are profiled (what data is inferred about us, how and why), and how and why voters are being targeted (e.g. based on our demographics, interests or other criteria). Voters should be given total insight into the process that puts them on specific target lists. If political parties and companies are profiling a voter a certain way, there are underlying assumptions being made about that voter based on their data. And unless voters know exactly what these entities base their targeting on, then the fairness of the whole process is questionable. For these reasons, it also needs to be clear who is involved and how – from the political groups to the companies they contract with.

The Electoral Commission could help to maximise fairness in online digital campaigning by taking into account data protection law in the interpretation of its mandate and regulatory activities.

Further, the above described transparency and fairness requirements should be applied beyond the strict electoral period – known as the regulated period in electoral law[13] –, and at all times in the Electoral Commission's exercise of its powers.

Q2 Does the Electoral Commission have the powers it needs to fulfil its role as a regulator of election finance under PPERA? It would be helpful if responses would consider the Commission's role in a) monitoring and b) investigating those it regulates.

The Electoral Commission does not have the powers it needs to accomplish its general functions. Under s.6(1)(f) PPERA 2000, the Electoral Commission is tasked with keeping under review political advertising in the broadcast and other electronic media. However, it is unclear how the Electoral Commission is able to carry out this reviewing function in the absence of a single, standardised source collating all political advertising. While some online platforms provide ads databases containing political ads (Facebook's Ad Library, Google's Transparency Report, etc), each online platform defines political ads differently, if at all.[14]

In order to properly meet its statutory duties, it is essential for the Electoral Commission to be able to keep a standardised and centralised database of all campaign adverts.[15] For this purpose, new powers are necessary for the Electoral Commission to be able to compel political parties, candidates and other political

[13] https://www.electoralcommission.org.uk/non-party-campaigners-where-start/does-your-campaign-activity-meet-purpose-test/purpose-test-regulated-period-early-uk-parliamentary-general-election
[14] https://privacyinternational.org/sites/default/files/2019-10/cop-2019_0.pdf
[15] https://fairvote.uk/wp-content/uploads/2020/01/Defending-our-Democracy-in-the-Digital-Age-APPG-ECT-Report-Jan-2020.pdf

actors to submit to it all political advertisements, whether off-line or online, along with a description of where the advertisement appeared, for how long, and to whom it was targeted. This would in turn make it easier for the Electoral Commission to enforce spending rules, and for researchers or members of the public to be able to conveniently consult ads.

Q3 What could the Electoral Commission do differently to allow it to perform its role as a regulator of election finance more effectively?

As has been stated in the answers to previous questions, the Electoral Commission could stand to improve its role as a regulator.

Heightened campaign spending reporting requirements

As outlined in the answer to Q1, the online political campaigning environment involves multiple processes and actors which are often invisible, and therefore escape scrutiny and oversight. 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."[16] 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.[17]

Privacy International recommends that campaign finance law, and the Electoral Commission, 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 party's services.[18]

While the Electoral Commission's search register provides some information as to the services contracted by political parties and candidates, it does not go far enough. Currently, the Electoral Commission's search register does not specify whether advertising spend relates to online or off-line political advertising.

---

[16] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[17] https://www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf
[18] https://privacyinternational.org/sites/default/files/2019-07/19.07.26%20APPG%20Submission_cover.pdf

Furthermore, there is some inconsistency as to the labelling of expense types: expenses classed as "advertising" and "market research/canvassing" could overlap in the online context. According to the Electoral Commission's Draft Code of Practice on qualifying expenses for political parties[19], the "advertising" spend category includes the cost of use or hire of a service to prepare, produce or facilitate the production and dissemination of digital or electronic advertising material. Conversely, "market research or canvassing" includes the use of data analytics to facilitate market research or canvassing. At present, because the production of electronic advertising material is so intertwined with data analytics (e.g. micro-targeting), market/canvassing expenses may easily be accounted for under the advertising category, and vice-versa.

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, on data sources, and how these were used e.g. which targeting techniques were deployed. The Electoral Commission should similarly 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.

Online repository of all political ads

In line with the increased need for transparency (as outlined in the answer to Q1), Privacy International supports the creation by the Electoral Commission of an online repository of all political ads. Solutions must enable meaningful transparency for users as well as enable effective scrutiny by researchers and civil society.

To do so, the Electoral Commission should compel political parties and other political actors to provide timely information on expenditure for online activities, including paid online political advertisements and communications. This should include information regarding companies assisting in online activities, including the amount spent on each companies' services. On the basis of the information received, the Electoral Commission should create a single, easily searchable and machine-readable, online database of all online and offline political advertisements (including any funded content) produced, with detailed reports of spend, reach and so on, which can then be cross-referenced against publicly available records held by online platforms themselves.

The Electoral Commission should also consider compelling online platforms to standardise the transparency required with regard to political advertisements, including the information described in the new section on digital imprints.

[19] https://www.electoralcommission.org.uk/sites/default/files/2020-04/Code%20of%20practice%20Political%20Parties%20UK%20April%202020.pdf

Digital imprints on ads

Transparency is also required for people as and when they see content, so as well as creating an online repository for political ads, the Electoral Commission should compel political parties and online platforms to label online campaign content as such to ensure that it is clear that something is campaign content, including information of who is behind the content (i.e. who paid for it), who created it, and why it is being targeted at an individual and on what basis. We note that the Electoral Commission has called for digital imprints to be included on online campaigning material since 2003.[20]

Regulation of data-driven processes behind political ad targeting

In close coordination with the ICO, and with the benefit of a public consultation process, the Electoral Commission should work towards developing binding guidelines specifying the ways in which political campaigns are and are not allowed to use data to target voters.

Q6 What are the Electoral Commission's strengths and weaknesses as a regulator of election finance?

Insofar as the solutions outlined in answer to Q3 are not implemented, the Electoral Commission will not be able to comprehensively carry out its duties under s.6(1)(f) PPERA 2000. This would constitute a weakness in its regulation of election finance.

Q7 Are the Electoral Commission's civil sanctions powers to fine up to £20,000 adequate?

No. Fines for electoral offences should be unlimited rather than subjected to a maximum of £20,000, an amount with little deterring potential.

Approaching this issue from a data protection perspective, previous experience tells us that weak enforcement powers create 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. For this reason, Data Protection Authorities were further empowered under GDPR to fine up to, the greater of €20million or 4% of global annual turnover. The Electoral Commission could no doubt benefit from being similarly empowered, and we note that the Commission has previously expressed the insufficiency of the £20,000 maximum fine.[21]

---

[20] https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/changing-electoral-law/transparent-digital-campaigning/report-digital-campaigning-increasing-transparency-voters

[21] https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/changing-electoral-law/transparent-digital-campaigning/report-digital-campaigning-increasing-transparency-voters

However, monetary penalties should not be the only sanction and consideration should be given to what type of behaviour can be prohibited as part of a sanction.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org