PRIVACY INTERNATIONAL

Submission to the House of Lords Select Committee on Democracy and Digital Technologies

September 2019

Table of Contents

About Privacy International

1. 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.

2. 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.

3. 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.

4. PI is increasingly concerned that democratic participation can be inhibited by novel and unhindered surveillance both by governments and companies. To safeguard our rights, earlier this year, we launched our work programme, Defending Democracy and Dissent[1], which aims to investigate the role technology plays in facilitating and/or hindering everyone's participation in civic society.

[1] https://privacyinternational.org/strategic-areas/defending-democracy-and-dissent

General

How has digital technology changed the way that democracy works in the UK and has this been a net positive or negative effect?

5. Digital technology has changed the way that democracy works around the world including in the UK. Digital technology and democracies are vast, intricate and complex and work in many ways and thus the situation is much more nuanced than classing these changes and the effect of them as a net positive or negative.

6. However, Privacy International is deeply concerned that democratic society is under threat from a range of players using digital technology to exploit our data in ways which are often hidden and unaccountable. These actors are manifold: traditional political parties (from the whole political spectrum), organisations or individuals pushing particular political agendas, foreign actors aiming at interfering with national democratic processes, and the industries that provide products and services that facilitate the actions of the others (from public facing ones, such as social media platforms and internet search engines, to the less publicly known, such as data brokers, ad tech companies and what has been termed the 'influence industry'[2]).

7. Personal data[3] and digital technologies play a fundamental role in this emerging way of seeking to influence democratic processes. Around the world, political campaigns at all levels have become sophisticated data operations. Whilst the use of data in political campaigning is not new, the scale and granularity of data, the accessibility and speed of the profiling and targeting which it facilitates, and the potential power to sway or suppress voters through that data is. The actors, tools, and techniques involved - who is using data, where are they getting it from, and what are they doing with it - vary depending on the context. Personal data can be exploited through a range of mediums to build profiles and to disseminate messages in a targeted manner, ranging from the use of text messages (SMS), to calls, to messaging apps (e.g. Whatsapp), to search results (e.g. through AdWords),

---

[2] See for example, the list of over 300 companies compiled by Tactical Tech: https://ourdataourselves.tacticaltech.org/posts/whos-working-for-vote

[3] Personal data as defined in the EU General Data Protection Regulation, which applies in the UK together with the Data Protection Act 2019, means "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

to campaign apps, to ad-supported platforms (e.g. Google, Facebook, Twitter, YouTube, Instagram) and websites, to television. A vast range of factors may play a role in the political content an individual sees, including where they've been (e.g. geotargeting - geofencing, beacons), what they've been doing (online and offline) what this says about their personality (e.g. psychometric profiling), and what messages they and people (like them) with particular traits have been most susceptible too (e.g. A/B testing).[4] This has consequences for the right to privacy and data protection, but also other rights including freedom of expression, association and political participation.

8. Data and technology are also becoming integral to the ways in which we vote - from the creation of vast voter registration databases, sometimes including biometric data, to reliance on electronic voting. Such voting processes are often implemented without sufficient consideration for their considerable privacy and security implications.

9. In UK, the concern and real harms are evident from the various reports and calls for action, including from civil society, journalists and regulators such as the Information Commissioner ("ICO") and the Electoral Commission. Parliament is also waking up to these threats and expressing concern, through the DCMS Committee on Disinformation, the All Party Parliamentary Group on Electoral Campaigning Transparency and the Joint Committee of Human Rights inquiry into the Right to Privacy (Article 8) and the Digital Revolution. These concerns continue to play out in political campaigns, and we are already seeing concerning practices ahead of a potential snap election in autumn 2019.[5]

10. As the political arena continues to adapt to the digital age, steps must urgently be taken to avoid the risks and negative consequences for democracy of the abuse of digital technology. For starters: existing legal frameworks (namely in relation to data protection and electoral law) must be implemented, enforced and strengthened; different actors must work together, from election officials and monitors, to data protection authorities and civil society; regulators must be empowered with sufficient powers and resources to hold to account; and actors at every level from political parties, to major social media platforms to data brokers and the wider 'influence industry' must improve their transparency efforts. This will in turn enable scrutiny by regulators, researchers, civil society and users.

[4] These techniques and examples of them are explained in detail here; together with the tools they use: https://ourdataourselves.tacticaltech.org/posts/inside-the-influence-industry

[5] https://www.politico.eu/article/general-election-boris-johnson-uk-facebook-digital-campaign-disinformation/

How have the design of algorithms used by social media shaped democratic debate? To what extent should there be greater accountability for the design of these algorithms?

11. Much focus of analysis of the role of social media in the democratic debate is on what we see online i.e. content, including for example disinformation and misinformation. Not enough consideration or acknowledgement is given to the role of the 'back end' of content - that is the design choices, algorithms and data which ultimately drives and shapes the content that we see and the knock-on role this can have on political campaigns and democratic debate. Most news sites, platforms, online retailers, social media platforms, music or video streaming services are now personalised, meaning that they deliver targeted content and adapt online experiences based on personal data they have collected about each visitor and inferences of individual's interests. As a result, the personal data that feeds into the largely automated architecture that is behind the content we see dictates much of our experience of the internet: when we search,[6] the posts that are pushed or promoted when we scroll through a social media feed,[7] what video is recommended next,[8] and what adverts we see, whether it is within an app, a platform or as we browse the web. How personal data is used (and often misused/exploited) in the backend is characterised by a concerning lack of transparency, fairness and accountability which too often falls short of existing data protection law. Privacy International outlined some of the harms of this in our response to the UK Government's consultation on online harms.[9]

12. 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 who, due to technical complexity or on the grounds of commercial secrecy, decline to explain how decisions are made. The few major platforms with their extraordinary reach therefore offer an easy target for people

[6] https://www.google.com/intl/en_uk/search/howsearchworks/algorithms/
[7] https://www.facebook.com/help/1155510281178725
[8] https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html
[9] https://privacyinternational.org/advocacy/3027/privacy-internationals-response-uks-open-consultation-online-harms-white-paper

seeking to use the system for malicious ends.".[10] 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[11]; Facebook's newsfeed[12]; or YouTube's recommendations[13]). These data targeting techniques risk exposing 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.

13. 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. For example, transparency, fairness and accountability requirements are already enshrined as principles in the EU General Data Protection Law ("GDPR") and those that use personal data are subject to the requirement of data protection by design and by default. However, Privacy International's view, as illustrated in our complaints against data brokers[14], is that many of the data practices, in particular profiling, employed by industry, are non-compliant with GDPR, particularly as personal data is processed with the absence of any legal basis, such as informed, freely given and specific consent. Design choices and default settings used by industry, including Facebook and Google, also fall short of the requirements of GDPR.[15]

---

[10] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[11] https://www.google.com/search/howsearchworks/algorithms/
[12] https://www.facebook.com/help/1155510281178725
[13] https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html
[14] See Privacy Internationals submissions complaining to data protection authorities in the UK, France and Ireland, setting out in detail why the practices of at least seven data brokers, credit reference agencies and ad tech companies fall below the requirements of GDPR: https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem
[15] Report by the Norwegian Consumer Council in June 2018, 'Deceived by Design' https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

14. Tackling these deficiencies and promoting proactive implementation and enforcement of existing requirements, including by imposing effective sanctions, is paramount to fostering democratic debate and protecting the democratic process in a digital era.

Online Campaigning

Would greater transparency in the online spending and campaigning of political groups improve the electoral process in the UK by ensuring accountability, and if so what should this transparency look like?

15. Transparency of online spending and campaigning by political groups, including digital advertising, is fundamental to ensure free and fair elections in the modern age and is the first step towards accountability.

16. 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 ad tech companies, data brokers, and other third-party companies that track people on websites and apps and combine this data with offline information.[16] 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[17] and updates to the DCMS Committee in July[18] and November[19] 2018 reference a number of such companies.

---

[16] See for example our complaints against data broker and AdTech companies (November 2018) https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem and recent reports (September 2019) on the sharing of data by mental health websites https://privacyinternational.org/campaigns/your-mental-health-sale and menstruation apps https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data

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

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

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

17. 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) – this should act as a starting place in terms of transparency. To date, there is a track record of widespread failure of compliance with these provisions (as Privacy International highlighted in submissions[20] complaining to the ICO and other data protection authorities about a number of companies in the data broker and ad tech sector). The data gathered and processed by these companies, including Acxiom and Experian, are often used for political purposes, including in the UK[21] and such companies often have products specifically aimed at the political market.[22] GDPR is over a year old and still in the early phases of enforcement, however, enforcement action is urgently needed and more needs to be done to ensure that all actors pro-actively implement and respect these obligations.

18. Transparency at every level must be proactive and up to date. Adequate, meaningful 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. It is currently extremely difficult to understand why you are seeing a political add on social media.[23] Such transparency should not be limited to advertising, but also include

---

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

[21] For example, the onboarding of Acxiom data to Facebook was credited with "Accurate targeting…essential to the [Conservative Party] campaign's success" in the UK General Election in 2015. "Partner segments were used for geographical targeting along constituency boundary lined, minimising wasted impressions and cousin ad delivery on adults who lived in … the most competitive constituencies. Custom Audiences (created from research and polling during the early days of the campaign) and Lookalike Audience were used to target messages to those with whom they would resonate" https://en-gb.facebook.com/business/success/conservative-party#u_0_0 and in relation to Experian, the example of a data broker company 'Emma's Diary' which provides advice on pregnancy and childcare, sold data to Experian specifically for use by the Labour Party, and was subsequently fined by the ICO : https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning/

[22] For example, Experian marketing material noting that Experian's Mosaic is used by the main political parties to profile the electorate, see for example, Experian's own marketing https://www.experianplc.com/media/news/2009/mosaic-uk-2009-experian-reveals-the-changing-face-of-uk-society or Oracle's 2019 Data Directory, for example advertises its i360 data for the US political and advocacy community, "of 190+ million active voters and 250+ million US consumers, with hundreds of data points on American adults", including categories such as "Swing Voters", "Likely Pro-Choice and Likely Pro-Life" http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf

[23] https://privacyinternational.org/long-read/3207/how-difficult-it-understand-why-youre-seeing-political-ad-social-media

the delivery of other content, such as the methods of curation, filtering, pushing, and recommendation of content.

19. 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 granular information on the sources of personal 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. Such transparency must be meaningful and useful for users as well as those seeking to scrutinise and hold to account, including civil society, independent researchers, journalists and regulators.

20. Political parties and other political actors should, as a minimum (a longer list is provided at the end of this document):

- 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 information on any targeting criteria used in the dissemination of such communications. This should be included as part of the communication but also publicly accessible, for example on their website.
- 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.

21. 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 (number of times an ad is shown) 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.

22. Recently, a variety of transparency tools have been developed, including extensions which users can add to their browsers, such as WhoTargetsMe[24] or recently in Argentina Publi Electoral[25] , 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[26] despite setting out some steps that could be taken to make the ad archives more effective.[27]

23. Furthermore, despite political parties and campaigns being required to provide certain information as noted above, their privacy policies do not provide enough detail. For example, see our analysis of the Conservative party leadership campaign.[28] A quick look at the policies of most of the UK political parties illustrate that they all by in large fall short. Further transparency was also a key part of the EU Code of Practice on Disinformation.[29] The failures to date, demonstrate the need for concrete action and proactive steps to ensure transparency, which is the first step towards any meaningful accountability.

24. As well as additional transparency on the use of data, from data sources to targeting criteria, Privacy International supports calls for additional disclosure 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.

25. 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

[24] https://whotargets.me/en/
[25] https://publielectoral.adc.org.ar/
[26] https://blog.mozilla.org/blog/2019/04/29/facebooks-ad-archive-api-is-inadequate/
[27] https://blog.mozilla.org/blog/2019/03/27/facebook-and-google-this-is-what-an-effective-ad-archive-api-looks-like/
[28] https://privacyinternational.org/long-read/3019/how-uk-conservative-leadership-race-latest-example-political-data-exploitation
[29] https://privacyinternational.org/news-analysis/2824/european-parliament-elections-protecting-our-data-protect-us-against

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.".[30] 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.[31]

26. 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.

27. To ensure effective monitoring the disclosure of campaign expenditure should be broken down into meaningful categories such as the 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 audience reached. 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.

What effect does online targeted advertising have on the political process, and what effects could it have in the future? Should there be additional regulation of political advertising?

28. A significant share of the content that people see on social media is either online advertising or content that has been promoted or sponsored. Every fifth post (or 20% of all content) on Instagram[32], for instance, is targeted advertising. Online targeted advertising is facilitated by a complex and opaque ecosystem that includes ad tech companies, data brokers, and other third-party companies that track people

[30] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
[31] https://www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf
[32] This can be measured, for example, by scrolling through and counting the number of ads per post on an Instagram account.

on websites and apps and combine this data with offline information. [33] On the surface, online advertising may appear harmless. In practice, however, it results in different concrete harms for people. Targeted ads can be discriminatory (someone might not be not shown a job because she is a woman or a loan because he lives in the wrong neighbourhood) and ads can seek to be manipulative (people can be served tailored information to target those that are most vulnerable) – therefore they may also seek to discriminate and manipulate in the political context. Secondly, the ecosystem of companies that collect, share and aggregate user data is so complex that it has become impossible for people to understand or control where information about them (their data) ends up, as well as the consequences this has for both them as an individual and society.

29. Examples of the harm caused by using online advertising for political purposes are plenty, and reports from the UK's Information Commissioner Office ("ICO"), including "Democracy Disrupted", have highlighted concerns with the use of personal data in political campaigning.[34] In 2018, the ICO fined Emma's Diary, a site offering pregnancy and childcare advice owned by Lifecycle Marketing Ltd, £140,000 for collecting and selling personal information belonging to more than one million people without disclosing in the site's privacy policy how it would be used.[35] Although Lifecycle denied the allegations, the ICO found that the company sold the data to Experian Marketing Services to build into profiles for use by the Labour Party, which targeted mothers in marginal seats with direct mail during the 2017 election campaign stating the party's intention to protect Sure Start children's centres. This is just one example, and there are many.[36]

30. On the question of whether further regulation is needed, the GDPR and the Data Protection Act 2018 ("DPA 2018") already provide the UK with tools to begin to tackle some of the issues of concern to the Committee, including political advertising. Privacy International first encourages measures to support the implementation and 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

---

[33] https://privacyinternational.org/long-read/2967/ad-supported-internet-broken-inefficient-and-privacy-nightmare-lets-fix-it

[34] https://ico.org.uk/media/action-wevetaken/2259369/democracy-disrupted-110718.pdf ; https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analyticsfor-political-purposes-update.pdf

[35] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning

[36] Here are just a few collated by Privacy International: https://privacyinternational.org/examples/political-advertising

practice, over one year on, a lot more still needs to be done and changes are only starting to take place.

31. However, there are also shortcomings related to the deterrence/enforcement legal framework in the UK. This includes an exemption for political parties, the need for a code of practice to be put on statutory footing, and that there be a form of collective redress (addressed later in this response).

32. The DPA 2018 contains an exemption for political parties that threatens 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 to 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.[37] A similar provision in the Spanish data protection law has since been declared unconstitutional[38] and another in Romania is the subject of a complaint to the European Commission.[39] Privacy International recommends that the Committee investigate how and for what purposes political parties in the UK are relying on this provision. Ultimately, we believe that the DPA 2018 should be amended to close this loophole.

33. Additionally, Privacy International supports the adoption of measures aimed at enhancing transparency in this field (as noted elsewhere in this response.). Given the failures of the actors involved to provide effective transparency (including in response to the self-regulatory EU Code of Practice) in relation to advertising, further, more prescriptive measures may be needed. However, given the difficulties in defining what constitutes political advertising and the many actors involved, effective ads transparency must go beyond obviously political ads and scrutiny not be limited to one particular platform. Solutions must enable meaningful transparency for users as well as to enable effective scrutiny by researchers and civil society.

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

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

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

Privacy and Anonymity

To what extent does increasing use of encrypted messaging and private groups present a challenge to the democratic process?

34. Privacy International believes that encrypted messaging is essential in securing and promoting the democratic process. Encrypted messaging allows the exercise of fundamental human rights, such as privacy and freedom of expression. This understanding should be the starting point of any discussion on the role of encrypted messaging in the democratic process. Communication security tools give individuals access to safe and private spaces for personal development where they can communicate without unwarranted interference.

35. Encryption is a key instrument to ensure that digital communications are protected from unwarranted interference, helping to preserve the right to privacy, as well as other rights, such as freedom of expression and freedom of association. As the UN Special Rapporteur on Freedom of Opinion and Expression highlighted "encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief."[40]

36. States have an obligation "to create and maintain a safe and enabling environment that is conducive to the exercise of the right to participate in public affairs."[41] Privacy International supports that any discussion regarding transparency should also envisage safeguards for end-to-end encrypted messaging. Undermining end-to-end encryption risks undermining democratic processes and open dialogue.

What are the positive or negative effects of anonymity on online democratic discourse?

37. As more of our lives are lived in the digital realm, communication security tools, such as encryption and anonymity tools and services, are increasingly important to the protection of human rights – particularly the right to privacy and the right to freedom of expression. Anonymity allows individuals to form opinions

[40] https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/_layouts/15/WopiFrame.aspx?sourcedoc=%2FEN%2FHRBodies%2FHRC%2FRegularSessions%2FSession29%2FDocuments%2FA.HRC.29.32_AEV.doc&action=interactivepreview

[41] https://www.ohchr.org/Documents/Issues/PublicAffairs/GuidelinesRightParticipatePublicAffairs_web.pdf

independently, free of inducement or manipulative interference of any kind.[42] As noted by the UN Special Rapporteur on freedom of expression, anonymity provides 'individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression.'[43]

38. Any interference with fundamental rights to privacy and freedom of expression, including any restriction to anonymity, must be lawful, necessary and proportionate to the achievement of a legitimate aim. These nuances must be considered in any efforts to enhance transparency online.

39. This applies also for political ads and issue-based ads, where the public interest of transparency and accountability of political actors is engaged, as well as the right to political participation (Article 25 of International Covenant on Civil and Political Rights), which includes the capacity of individuals to form opinions, including political opinions, without undue interference.

40. Privacy International has been advocating for increased transparency in political advertising. Given the granularity with which advertisers are able to target users on Facebook, Google, and Twitter, the companies must provide much more information about why users are seeing an ad.[44] However, Privacy International also recognises that in some cases, there is a legitimate need to advertise anonymously, for example, due to risks of violence or other human rights abuses. Options of how this could be modelled should be explored. It is important that companies understand the contexts in which they operate and build strong independent national teams.

[42] Human Rights Committee, General Comment No. 25: The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service (Art. 25), vol. CCPR/C/21/Rev.1/Add.7, 12 July 1996.
[43] Report of the UN Special Rapporteur on freedom of expression, UN Doc. A/HRC/29/32.
[44] https://privacyinternational.org/long-read/3207/how-difficult-it-understand-why-youre-seeing-political-ad-social-media

Democratic Debate

To what extent do you think that there are those who are using social media to attempt to undermine trust in the democratic process and in democratic institutions; and what might be the best ways to combat this and strengthen faith in democracy?

41. As noted elsewhere in this submission, social media is part of a long tail of actors involved in and linked to political campaigns, and the actors seeking to influence the democratic process are manifold.

42. The starting place in distinguishing those seeking to undermine the democratic process and failing to comply with existing legal safeguards is transparency together with implementation and enforcement of existing legal frameworks. There is a need for measures tailored to each actor that may engage in or facilitate detrimental behaviour (e.g. political parties, social media companies, and the data brokers, ad tech companies and others in the 'influence industry'). There is also a need to empower regulators and enforcement bodies, with sufficient resources to independently investigate and hold to account, this includes acting on calls for change, for example enshrining a Code of Practice on Political Campaigning in law and updating electoral campaigning law for the digital era. Without such proactive steps and intervention as illustrated throughout this submission, current practices risk undermining trust in the democratic process.

Misinformation

What might be the best ways of reducing the effects of misinformation on social media platforms?

43. As noted elsewhere in this submission, whilst significant efforts have been made to identify 'misinformation' and 'disinformation' and to propose solutions such as 'take downs' and 'fact checking', these are limited to the content of the information. Privacy International believes that equal or more attention should be paid to understanding and enforcing the laws related to the way content is distributed and targeted (the 'back end').

Technology and democratic engagement

How could the Government better support the positive work of civil society organisations using technology to facilitate engagement with democratic processes?

44. One way in which the Government could better support civil society is to introduce collective redress mechanisms that empower civil society to take action to hold to account those who are using technology to undermine the democratic process. No sufficient mechanism is currently available and was explicitly excluded from the DPA 2018 despite being an option in the GDPR.

45. 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.[45] This mechanism has been used by Liberty and Southhall Black Sisters to challenge police data sharing for immigration purposes.[46]

46. 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 people more than others. Particularly when it comes to abuse in the political context, much of the work done to identify and expose bad practices has been the result of the dedication of researchers, journalists and civil society.

47. 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

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

the European Data Protection Supervisor[47] and by Privacy International.[48] In spite of this, and cross-party support, in particular in the Lords, Article 80(2) of GDPR was not implemented in the DPA 2018. Instead, it will be the subject of a review 30 months from the DPA 2018 having come into force (section 189(2)(c) of the DPA 2018).

48. Privacy International encourages the Committee to consider mechanisms for the introduction of 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 Committee should engage with the promised review of Article 80(2) in 2020.

How can elected representatives use technology to engage with the public in local and national decision-making? What can Parliament and Government do to better use technology to support democratic engagement and ensure the efficacy of the democratic process?

49. A key starting point for elected representatives is to lead by example. As set out above, large platforms, together with the vast 'influence industry' from data brokers, to ad tech, to the providers of campaign tools and services have much to answer for. However, political parties as the users of these services must shoulder some responsibility and take steps now to demonstrate a commitment to respecting people's rights. Here are ten steps that elected representatives should abide by in their own and their party's political campaigning.

1. Be transparent about data processing activities, including identifying the mechanisms used to engage with voters (e.g. social media, websites, direct messaging);
2. Be transparent about collection of people's data and the sources of this;
3. Be transparent on political ads and messaging. Ensure that the public can easily recognise political messages and communications and the organisation behind them. Make available information on any targeting criteria used in the dissemination of such political messages;
4. Publish a complete, easily accessible and easily understandable list of any campaign groups which a candidate/party has financial or collaborative

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

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

campaigning relationships with, including all third parties and joint campaigners;

5. Adopt and publish data protection policies and carry out and publish data protection audits and impact assessments;
6. Ensure have a legal basis for each use of personal data (including any special category data such as those revealing political opinions);
7. Be transparent as to the companies contract with as part of campaigns both to obtain data and to further process data, including profiling and targeting, such as data brokers and political advertising companies as well as which companies are providing campaign tools/ software and which products are being using;
8. Ensure that any third party used for campaign activities also complies with data protection laws;
9. Make publicly available timely information on expenditure for online activities, including paid online political advertisements and communications. This should include information regarding which companies have assisted in online activities, including the amount spent on each companies' services;
10. Facilitate the exercise of data rights by individuals (including providing information about how their data is processed and providing timely access to it).

50. The Government and Parliament can ensure that electoral law and data protection law are updated to make the above as legal requirements and give independent regulators such as the Information Commissioner's Office and the Electoral Commission sufficient powers and resources to enforce them. Resources must include human, financial and technical. This requires, from an electoral law perspective, at a minimum ensuring that there are sufficient sanctions in place; that online campaign details are provided in a sufficiently timely and granular manner and requiring transparency of the third parties with which campaigns contract as well as their targeting activities. From a data protection perspective, as a minimum, this requires implementation and enforcement of the existing data protection framework, giving effect to a new statutory code of practice (on which the ICO is currently consulting), narrowing the exemption for political parties in paragraph 22 of Schedule 1 to the DPA 2018 and empowering civil society to take collective action under Article 80.2 of GDPR (as discussed above).

Appendix – Resources of Interest

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