Challenging Data Exploitation in Political Campaigning

PI Recommendations

June 2020

privacyinternational.org

ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice.

So, join our global movement today and fight for what really matters:
our freedom to be human.

Photo by Fred Moon on Unsplash

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

CONTENTS

EXECUTIVE SUMMARY

Around the world, political campaigns are becoming increasingly reliant on the exploitation of people's data for political gain.

Effective safeguards that reflect these changes in digital campaigning both now and looking into the future are needed. The form of legal and regulatory frameworks and responses may differ. However, all actors involved - governments, regulators, companies and political parties - must take measures to resist the current race to the bottom.

Privacy International (PI) considers that there are certain baseline safeguards that should be in place.

In summary:

1. More transparency is needed from all actors involved in digital political campaigns, including political parties and all companies, in order to shed much needed light on data gathering practices, how such data is used, in particular for profiling, and then how such profiles are used to target messaging. This transparency is vital to understand how political campaigns work now and may work in the years to come, who campaigns work with, what data and tools they use and how. This transparency should in turn lead to appropriate limits being put in place and those that fail to comply being held accountable.
2. Transparency is needed for voters, for regulators and for researchers. All online and offline advertisements should be publicly available, easily searchable and machine-readable, with detailed information including who received what, why and under which circumstances.

3. Comprehensive data protection laws must be implemented and enforced. Any loopholes that can be exploited by political campaigns must be closed. Data protection authorities should issue binding enforceable guidance on the use of data in political campaigning and carry out proactive investigations.
4. Electoral laws need to be updated for the digital age. They must reflect that digital political campaigning takes place outside the strict electoral period and require detailed and timely reporting on campaign advertising and financing.
5. These legal frameworks must provide effective redress (both individual and collective) and meaningful sanctions if they are violated.
6. Regulators, judicial and other supervisory/oversight authorities, in particular those responsible for data protection and electoral law, must have sufficient independence and adequate resources (both technical, human and financial) to enforce the law.

These recommendations are addressed below to three sets of actors:

I. Governments, Legislators and Regulators;

II. Political parties and political campaign groups ; and

III. Companies, that is the "ecosystem" of companies involved in political campaigning.

INTRODUCTION

Democratic engagement is increasingly mediated by digital technology, from campaigning to election results transmission. These technologies rely on collecting, storing, and analysing personal information to operate. They raise novel issues and challenges for all electoral stakeholders on how to protect our data from exploitation.

The entire election cycle is increasingly data dependent. This is particularly the case with political campaigns which are ever more digital and data driven. This campaign environment presents novel challenges due to the scale and range of data available together with the multiplicity, complexity and speed of profiling and targeting techniques. All of this is characterised by its opacity and lack of accountability. Existing legal frameworks designed to curtail this exploitation often also fall short, either in substance or enforcement.

These are concerns that have been raised by various actors around the world in recent years – from civil society, to regulators to parliamentarians. For example, in March 2018, the European Data Protection Supervisor (EDPS) released an opinion explaining that data harvesting and machine learning systems were having serious impacts on civic engagement and political decision-making.[1]

NGOs, researchers and regulators have been focusing on this issue, but its complexity and the profound lack of transparency makes mapping and understanding the dynamics at play challenging. Much recent debate has focussed on the content of election-related digital communications, e.g. 'fake news' and disinformation, particularly in the form of political adverts and messages we see on social media. At PI, we are interested in what is "behind the curtain" - what data has been collected and inferred about you that has resulted in you being targeted with this content.

[1] EDPS Opinion 3/2018 on online manipulation and personal data, March 2018: **https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf**.

Through the amassing and processing of vast amounts of data, by platforms, data brokers, and other intermediaries and trackers, individuals are profiled based on their stated or inferred political views, preferences, and characteristics. These profiles are then used to target them with news and other content aimed at influencing and manipulating their view, which raises questions as to the transparency, fairness and accountability of both the data use and the campaign. This phenomenon in turn may lead to a number of harms including harms to individual autonomy, to civic participation, and other more diffuse harms to the integrity of the political process that may include political polarization.

In attempting to address these issues, it is essential to examine the relevant legal frameworks in place, if they offer sufficient safeguards, and if not what the gaps are. There are a range of relevant legal frameworks to consider, from electoral law, to political campaign financing law, to broadcasting and media regulation, advertising rules and data protection law. However, often these frameworks have not been updated to sufficiently address changes in digital campaigning, are disjointed, or lack teeth, an issue exacerbated by a lack of resources, coordination and enforcement action. As a result, they risk not being effective.

Effective legal frameworks are necessary as companies' own efforts do not go far enough, are applied unequally around the world, and ultimately have the companies economic incentives at heart.[2] Responses so far have primarily focused on regulating content, e.g. requesting political or issue-based content takedowns, requiring the introduction of fact-checking or curbing anonymous posting. Well-intentioned as they might be, and notwithstanding the rights implications, including to freedom of expression, these efforts have failed to address the underlying data aspects, perhaps because doing so strikes at the core of many companies' business models. It is more important than ever for us to consider the ways in which data is used in the context of modern democratic societies and to take steps to curtail its exploitation. Left unchecked, such exploitation is not only highly privacy invasive and raises important security questions, but it also has the potential to undermine human dignity, social cohesion and faith in the democratic process.

[2] Privacy International, Social media companies have failed to provide adequate transparency to users globally, September 2019: **https://privacyinternational.org/node/3244.**

Political campaigns vary depending on context, as does *who* is using data in campaigns, *what* the sources are and *how* that data informs campaign communication. There is still a deep gap in understanding as to how this is playing out around the world.[3] The form of legal and regulatory frameworks and responses may also differ. However, we need effective safeguards that reflect changes in digital campaigning both now and looking into the future. We need to see actors around the world, from governments, regulators, platforms to political parties, taking measures to resist the current race to the bottom.

[3] Dommett, K., "Data-driven political campaigns in practice: understanding and regulating diverse data-driven campaigns", (2019) *Internet Policy Review*, 8(4): **https://policyreview.info/articles/analysis/data-driven-political-campaigns-practice-understanding-and-regulating-diverse-data**.

I. GOVERNMENT, LEGISLATORS, REGULATORS

Around the world, laws and regulatory mechanisms are proving insufficient to provide safeguards for the way that digital campaigning has developed. Where frameworks are in place, they suffer from a vast enforcement gap. Legislators and governments must develop, strengthen and enact updated legal frameworks. Those must then be enforced by those empowered to do so, courts, oversight bodies and regulators.

As a starting point, human rights, data protection and electoral law frameworks should be in place, strengthened and implemented.[4] Among other things, this requires well-resourced, independent oversight bodies to enforce them:

- Regulators must be empowered to provide clear and binding guidance, take action (both proactively and in response to complaints) and enforce the law, have the ability to conduct their work without external pressure and with the ability to request information from and if necessary take action against all parties involved in the electoral cycle.
- Regulators must be given the necessary resources (financial and capacity, including technical) to take such action.
- There is a need for joint cooperation and enforcement between regulators at national, regional and international levels. Threats to elections come from diverse actors and require the engagement of multiple regulators as well as coordination among them.

[4] Other laws including advertising, telemarketing/ anti-spam, communications and cybersecurity may also come into play.

A. DATA PROTECTION LAWS

The unauthorized processing of personal data infringes the right to privacy. Data protection laws are fundamental to enforcing this right. Over 130 countries around the world have now enacted data protection legislation of varying strengths.

- National laws should recognise fundamental human rights, this includes the human right to privacy (including as part of it or as an additional right, the right to data protection), as well as other human rights, such as the rights to freedom of opinion and expression, to seek and receive information, to freedom of thought, to freedom of association, and to political participation.
- In addition, a modern, comprehensive data protection law should be in place with an independent, sufficiently resourced data protection authority.
- The data protection law should be regularly reviewed to ensure its provisions are up to date and effective in addressing the challenges posed by the application of new technologies, including in the electoral context.
- Each national data protection authority should issue a binding code of practice, code of conduct or equivalent that applies to all actors involved in political campaigns, with any violations being subject to appropriate enforcement action.

1. Personal data

The definition of personal data must be sufficiently broad to encompass the different forms of data that may be used in political campaigning. It must include data that does not directly identify (including online identifiers such as cookies and Advertisement IDs) but that may be related back to an individual.[5] Personal data must also cover inferred data, i.e. data that is inferred about an individual from other data, for example, through profiling.

There is a risk that some of the processing of data used in political campaigning will seek to circumvent the definition of personal data, through for example, claiming profiles or segments are not personal data if they are created from aggregated data or that apply to groups/ households as opposed to individuals. However, these data can then be associated with individuals and may enable political actors to reach individuals without actually having their data. Another attempt to circumvent this definition might be to argue that the data is anonymous because it does not contain a clear and unique identifier such as a name or an email address. Much research has demonstrated, however, that individuals can be identified from just a few seemingly anonymous data points.[6] The law must be clear that pseudonymous data, from which people can be re-identified, is covered by the definition of personal data.

[5] See section on definitions in Privacy International, Data Protection Guide: **https://privacyinternational.org/data-protection-guide.**

[6] Whether, location data, see de Montjoye, Y., Hidalgo, C., Verleysen, M. *et al.,* "Unique in the Crowd: The privacy bounds of human mobility", (2013) *Scientific Reports* vol. 3, Art. No. 1376: **https://doi.org/10.1038/srep01376**. For browsing history, see, for example, the 'anonymous' browsing habits of over 3 million Germans were used to identify a judge's porn preferences and the medical history of a doctor. Alex Hern, "'Anonymous' browsing data can be easily exposed, researchers reveal", August 2017: **https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers.**

2. Sensitive personal data

Most data protection laws around the world give special protection to personal data revealing political opinions, as well as other protected characteristics such as race, health and sexual orientation. This extra protection is in recognition of the sensitivity of this data and significance of the consequences of its use. As more and more data is collected, observed and inferred about individuals, more can be revealed about individuals' political opinions even where such opinions are not explicit.

- Political opinions/views should be given special protection as sensitive data.
- Protections for sensitive data must cover data that reveals sensitive data, including political views, i.e. not just overtly or explicitly political opinions.
- There should be a prohibition on processing this data unless very specific and narrow conditions are met. (See the below section on lawfulness for a description of those conditions.)

3. Profiling and Microtargeting

Profiling is the use of data to evaluate, analyse or predict a person's traits or behaviour. Profiling both uses and creates personal data, meaning that organisations, including those an individual may never have heard of, learn about and infer information about and categorise people according to their habits and personality, including political beliefs. Profiling is at the core of the business models of AdTech companies, data brokers and platforms and is now rampant in digital campaigning.[7]

Data protection law should cover profiling. This includes where profiles are developed based on aggregated data but then associated with individuals, as well as where tools enable political actors to reach individuals based on certain data points without actually having their data (e.g. through retargeting, using

[7] See for example, PI, Why we're concerned about profiling and micro-targeting in elections, April 2020: **https://privacyinternational.org/news-analysis/3735/why-were-concerned-about-profiling-and-micro-targeting-elections** and PI, Hiding in plain sight—political profiling of voters, December 2017: **https://privacyinternational.org/blog/742/hiding-plain-sight-political-profiling-voters**.

tools such as custom audiences and lookalike audiences[8] or equivalent). It must cover both the input and the output data, including whether sensitive output data is generated from non-sensitive input data.

Profiles can then be used to target people, with content, advertising and messaging, at an ever more granular, personalised level (based on their perceived preferences and personality traits). This practice is known as micro-targeting. Profiling and the micro-targeting it facilitates can be described in the following stages:

(a) collecting data (data is often collected through hidden means, such as trackers, and from a range of sources, such as data brokers, voter registries, social media etc)

(b) dividing voters into segments based on characteristics such as personality traits, interests, background or previous voting behaviour, also known as profiling;

(c) designing personalised political content for each segment; and

(d) using communication channels to reach the targeted voter segment with these tailor-made messages'

The use of data in each of these stages – the gathering, the profiling and the targeting- should be covered and limited by data protection law. Below in the section on further regulation, we cover whether additional protections and/or specific limitations for micro-targeting should be in place.

[8] Custom audiences and lookalike audiences are the language used by Facebook, for example see Facebook Audiences page (**https://en-gb.facebook.com/business/help/572787736078838?id=176276233019487**) where it describes either uploading data to reach or exclude a specific audience, or reaching an audience on that platform similar to your existing audience. Google and Twitter have equivalents, as do a range of other platforms. For further information, see PI, Apart from Google, Facebook and Twitter, what are other platforms doing about political ads?, April 2020: **https://privacyinternational.org/long-read/3703/apart-google-facebook-and-twitter-what-are-other-platforms-doing-about-political-ads**.

4. Transparency

Data protection law must mandate transparency of why and how data is used, as well as the potential consequences of this. The principle is bolstered by individuals' right to information, and that right should receive detailed articulation in any data protection regime. In the political campaigning environment, even more detailed transparency requirements should be articulated in a binding code of practice and/or electoral law.

This is particularly important given the prevalence of 'invisible' or 'hidden' processing in the political context. The current lack of transparency by political campaigns and those companies they work with is a huge obstacle to scrutinising their practices, further eroding trust in the campaigning environment and the electoral process.

We should know how our data is being used at every stage of political campaigning. From collection - what data is being gathered about us (e.g. whether we've voted before, our phone number, email or online identifiers), from where (e.g. voter lists, data brokers or social media), to how we are profiled (what data is inferred about us, how and why), and how and why we are being targeted (e.g. based on our demographics, interests or other criteria). It also needs to be clear who is involved and how – from the political groups to the companies they contract with.

Those involved in political campaigns should be required by law to proactively provide this information. At the very least, it should be available in their publicly available privacy notices and in response to access requests by individuals.

The law must require that for all actors it is clear:

- Who is using personal data.
- What personal data they are using.
- The source of the personal data.
- How they will use personal data and with what justification (purposes of processing and the legal basis).

- Who the data will be shared with, for what purpose, and if so, what safeguards are in place.
- The period for which the personal data will be stored and why.
- Information about any profiling, including the input data used to create the profile, information on the profile, the details of any segments as well as the significance and envisaged consequences.
- Information about any automated decision-making, including profiling, including meaningful information about the logic involved, the significance and envisaged consequences of the processing as well as factors taken into account as part of the decision-making process and their respective weight.

National laws and regulations should require companies and political campaigns to be transparent regarding online political advertisements and communications and how they are targeted. To avoid difficulties over what is considered political or not, and to ensure that campaigns do not seek to circumvent this requirement, detailed transparency should be provided for all ads, not just political ones. The failures of voluntary transparency to date show that transparency must be required by law. For more detail about what transparency in the political context should look like in practice, see the details in the section on transparency for Political Parties and Campaign Groups and the section on transparency for Companies.

5. Lawfulness

Data protection law provides the framework within which data can be used. This includes the requirement that data only be used in a way that is lawful. Data protection law does not exist in a vacuum and must be applied in a manner consistent with all other applicable legal requirements including human rights, anti-discrimination laws, laws protecting confidentiality of communications, and electoral laws, to name a few.

Processing of personal data must also have a lawful basis i.e. a legal justification under data protection law, where a limited number of justifications should be clearly set out. For example, a lawful basis may be free, specific, informed and unambiguous consent. Other bases may be set out in law where the processing is necessary, i.e. the least intrusive way of achieving a legitimate aim. These legal bases should be limited and explicit, especially in the political campaign environment.

Every stage of use of data in political campaigning – collection, profiling, sharing, targeting, re-using etc – must have a legal basis. If it does not, then the activity should not be taking place.

As noted above, the assessment of the lawfulness of data processing may involve the consultation of multiple legal instruments, not just data protection law. For example, if the method of data collection involves data from a device, then it may be covered by an electronic privacy law or equivalent which may limit the available legal bases. Similarly, relevant guidance, opinions and cases should be a point of reference: for example, there are many situations, including profiling, where it has been stated clearly by data protection authorities[9] that given the intrusive nature of the processing, the legal basis known as 'legitimate interest' is unlikely to be valid.

The conditions for using sensitive personal data such as personal data revealing political opinions should be even more stringent in order to prevent abuse.

Data protection law should not provide exemptions that can be exploited in political campaigning, including through use of broad and undefined terms.

[9] See for example, Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of the Directive 95/46/EC: **https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf**; and Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679: **https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053**.

Political loopholes in data protection law

There are some ways in which the European Union's General Data Protection Regulation (GDPR) derogations have been implemented at national level that undermine the requirements for lawful processing in the political context.

For example, in the UK, a broad exemption for democratic engagement was introduced in section 8 of the Data Protection Act 2018, and a condition in paragraph 22 of Schedule 1 to the Data Protection Act 2018 allows political parties to process personal data revealing political opinions if necessary for their political activities.

Similar exemptions introduced in Spain and Romania have already been challenged. The Spanish law allowed political parties to use personal data obtained from web pages and other publicly available sources when conducting political activities during election campaigns.[10] The provision further authorised political parties to send citizens messages via social media and "equivalent media" without consent. The data protection authority issued an opinion[11] arguing for a restrictive interpretation to this provision, followed by a circular[12] establishing the criteria to evaluate the legality of campaign activities. The provision was then invalidated by the by the Spanish Constitutional Court in May 2019.[13] In Romania the provision is part of a pending complaint before the European Commission.[14]

[10] See Article 58 bis 1, Ley Organica 5/1985, 19 June, Regimen Electoral General, Spain: http://noticias.juridicas.com/base_datos/Admin/lo5-1985.html.

[11] See the Opinion of the Spanish Data Protection Authority (AEPD) on the use by political parties of data relating to political opinions, December 2018: https://www.aepd.es/sites/default/files/2019-09/2018-0181-tratamiento-datos-opiniones-politicas-por-partidos-polticos.pdf.

[12] See the Circular 1/2019 from the AEPD on the processing of personal data relating to political opinions and the sending of electoral propaganda through electronic means, March 2019: https://www.boe.es/boe/dias/2019/03/11/pdfs/BOE-A-2019-3423.pdf.

[13] Summary of decision of the Spanish Constitutional Court , May 2019: https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_074/NOTA%20INFORMATIVA%20N%C2%BA%2074-2019.pdf.

[14] Complaint by Romanian civil society organisation APTi to the European Commission, https://www.apti.ro/sites/default/files/Complaint%20on%20Romanian%20implementation%20of%20the%20GDPR%20-%20ApTI.pdf.

6. Fairness

Fairness is another key principle of data protection that is relevant in the political campaigning context.

Fairness is intimately linked with individual's reasonable expectations as to how their data may be used. Numerous surveys show that people may be unaware of developments in digital campaigning.[15] If they are aware, they are often extremely concerned. Thus, the way data is increasingly used in digital campaigning may not be within individuals' reasonable expectations because they are either unaware of it or because they are aware of it but find it unacceptable, thus raising questions of fairness .

It is important to emphasise that the apparent normalisation of the use of many campaigning methods in the online world coupled with lack of enforcement action against the majority of actors does not mean that the processing is fair.

If processing is unfair then it should not be going ahead.

7. Purpose Limitation

The purpose limitation principle requires that the purpose of the collection of personal information should be specified at the time of collection. The information may not be further processed in a manner incompatible with those purposes and whenever there is a change of purpose it must be specified.

[15] For example, in the US, John S. and James L. Knight Foundation and Gallup survey published in March 2020 found that 72% of respondents say that internet companies should make no information about its users available to political campaigns in order to target certain voters with online advertisements. Justin McCarthy, "In U.S., Most Oppose Micro-Targeting in Online Political Ads", March 2020: **https://news.gallup.com/opinion/gallup/286490/oppose-micro-targeting-online-political-ads.aspx**. In the UK, research by Harris Interactive, commissioned by the Information Commissioner into online advertising found that 63% of the 2,300 participants indicated that they found it acceptable that ads funded free content; however, when they were given an explanation of how AdTech, in particular Real Time Bidding works, this feel to 36%. Michael Worledge and Mike Bamford, AdTech Market Research Report, March 2019: **https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf**.

This principle illustrates that digital campaigning cannot be a data free for all. As much of the data currently used in political campaigning was not intended for this purpose, it should not therefore be being used in this way.

8. Data Minimisation

Developments in digital political campaigning go hand in hand with the pervasive assumption that more and better data on the electorate can help win elections and consolidate political power. This race for data maximisation directly contradicts the principle of data minimisation: that data should only be adequate, relevant and limited to what is necessary in relation to the purpose.

9. Accountability

a. DPIAs

Data protection impact assessments (DPIAs) should be required in the context of digital political campaigning, particularly where methods and techniques such as profiling and micro-targeting are being deployed. Such assessments should not be a tick box exercise, rather an opportunity to fully assess the risks and consequences and avoid going ahead with exploitative processing. The law should provide that these assessments be made available to regulators but also include a presumption in favour of making these publicly available.

b. Obligations on processors

The law should be clear as to the obligations on processors of personal data. There is a risk in the digital campaigning environment that many third parties seek to shirk responsibility through claiming the role of processor, as opposed to the role of data controller. On the facts this may not be the case, but where it is, it is essential that the law also provides clear obligations and that these are elaborated on in a code of practice.

c. Data Rights

Data rights, including the right to information, to access, to amend, to object and to delete are key to a comprehensive data protection framework and aim to afford some degree of control to individuals over how their data is used. The importance of these rights is highlighted in the political context, where it is vital that individuals are provided with information about what data political campaigns have about them and how those campaigns are using the data, including to target individuals. Among other rights, individuals must be able to object to such use. These rights must be free to exercise and require a timely response.

d. Audits

The law should empower regulators to scrutinise political campaigns and third parties from platforms to digital campaign companies, including through audits both before and after elections.

e. Codes of Conduct/Practice

The law should empower regulators to develop and implement codes of conduct/ practice on political campaigning. The law should give these teeth by making them statutory and thus binding and enforceable. Data protection authorities should consult widely in the development of such codes and review them regularly. Where the law does not provide for such statutory codes, then as a very minimum regulators should provide guidance on political campaigning setting out in particular what behaviour is not permissible.

B. ELECTORAL LAWS

Electoral laws, as a category, include the laws regulating the running of elections as well as aspects such as voter registration, access to voter records, registration of political parties and candidates, and campaigning, including financing (donations and spending), transparency, advertising oversight, and the media.

1. Update electoral laws for the digital age

Too often these laws have not been updated for the digital age. For example, the same safeguards that apply to print and broadcast in elections may not yet apply in a digital environment.

Review and reform are needed if electoral laws are to be effective at regulating digital campaigning and ensure transparency, fairness and accountability in the electoral process. This includes requiring more transparency of campaign financing and advertising; increasing the frequency and granularity of reporting requirements; and strengthening the powers of regulators.

It is also important that electoral laws are not interpreted in a vacuum. Given the increased use of data and data driven technologies in the electoral cycle, consideration should be given to the interplay with data protection law.[16]

[16] For example, in Brazil the Superior Electoral Court regulations incorporates some provisions of the data protection law as a result of the interpretation of the electoral law in light of data protection principles and rules, for more information see summary by InternetLab, February 2020: **https://www.internetlab.org.br/en/information-politics/working-through-information-politics-achievements-and-prospects/**.

2. Scope of laws regarding the use of data for political campaigning purposes

It is important to note that political campaigning, with the potential for exploitation of people's data, is not limited to the run up to elections or referenda. Such laws must apply to political campaigning beyond the strict election period and cover the full electoral cycle. The misuse of personal data for political manipulation can happen at all times, and not just around elections.[17] Focusing only on the election period and just on the political parties or official candidates will miss a significant and growing phenomenon, which directly influences democracy and public discourse.

3. Transparency

Transparency is the first step towards fairness and accountability. Recognition of the importance of how much money is spent in political campaigns, how it is used and where it comes from should mean that there are specific requirements regarding campaign finance, covered below.

However, as campaigns become more digital, more transparency of the digital activities involved in campaigning and what such campaigns look like (including all the actors involved) is also needed. To ensure that what happens in practice ties up with the information provided by campaigns, electoral laws should also facilitate the regulator carrying out audits before and after an election.

[17] Targeting may, for example, seek to influence people's political views more broadly, or demand they support or oppose a political issue, such as a draft law or a key policy vote in Parliament. For example, the United Arab Emirates and Saudi Arabia used online advertising and social media campaigns to seek to influence US policy on Qatar. Josh Wood, "How a diplomatic crisis among Gulf nations led to a fake news campaign in the United States", *GlobalPost*, July 2018: **https://www.pri.org/stories/2018-07-24/how-diplomatic-crisis-among-gulf-nations-led-fake-news-campaign-united-states**; and in the US a senator targeted Facebook Ads a specific Department of Interior building in a bid to seek to convince officials to change their opposition to the construction of a road. Kashmir Hill, "How a Senator used Facebook ads to influence employees in a single D.C. building", *Splinter*, April 2016: **https://splinternews.com/how-a-senator-used-facebook-ads-to-influence-employees-1793856310**.

There are specific steps that should be taken to provide transparency by political parties and campaigns and companies (see the section on transparency in the section covering Political Parties and Campaign Groups and the section on transparency covering Companies.)

Suggestions for improving transparency overall include:

- A publicly accessible database of all entities that have bought access to the electoral register and for what purpose.
- All online and offline advertisements should be submitted to the electoral authority and publicly available, through the creation of a single online database of political adverts, which would be easily searchable. This should include copies of all leaflets and digital ads (including any funded content) produced, alongside audience details (who received what and why), and detailed reports of spend, reach and so on, which can then be cross-referenced against publicly available records held by online platforms themselves.
- 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.
- As part of the above, laws and regulations should require the disclosure of information on any targeting techniques and criteria used by political parties, platforms and others in the dissemination of political communications.
- Any actor taking part in political campaigning (including private companies) should also provide transparency in regard to its political affiliation. For instance, this could be done by disclosing political clients. This is important given the use of third parties or groups that might not be overtly affiliated to carry out many campaign activities.
- For fairness and accountability, transparency has to be provided throughout the full electoral cycle and not just in the immediate run up to an election.

4. Campaign finance laws

a. Timely reporting

Campaign finance laws should require timely reporting of spending on online campaigning as well as donations and funding obtained online. In order to make it meaningful and actionable, this reporting should be near real-time.

b. Detailed and meaningful transparency on funding and spending

Information provided by political campaigns should be sufficiently granular to promote transparency and accountability.

Therefore, reporting requirements by political campaigns must include detailed reporting – both to the electoral authority and publicly – broken down into meaningful categories covering digital campaigning activities, including spending on types of content, on which companies, on which data sources, and how these were used e.g. which targeting techniques were deployed.

This should include information regarding which third parties, if any, have assisted the political actors with their online activities, for what purpose, and the amount spent on each third party's services.

From this information, it should also be clear what the total spend was per actor, to avoid campaigns seeking to avoid reporting requirements through multiple smaller spends.

Transparency is also required for people as and when they see content, so as well as providing online databases of ads and reporting to regulators, campaign content should be labelled as such to ensure that it is clear that something is campaign content, 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.

C. REMEDIES AND PROCEDURES

1. Effective Redress (Individual & Collective)

An independent complaint mechanism is necessary to ensure that electoral processes are free and fair and that all actors involved are accountable.

As elections and democratic processes (such as participation in political campaigns) are manifestations of the enjoyment of fundamental human rights, governments have legally binding obligations to ensure that individuals have an effective right to redress any violations of their rights in this context.

Considering the collective nature of democratic processes and their effects, and the complexity of digital campaigning and the related issues, there is also need for collective redress mechanisms that empower civil society to take actions to hold to account and seek redress. Regulatory regimes are stronger and more effective if civil society can act in the public interest to bring complaints before regulators and courts. Complaints before regulators should bear no costs and there should be caps on the costs involved in bringing such actions before courts. 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.[18]

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.

[18] PI, Why we need collective redress for data protection, January 2018: **https://privacyinternational.org/news-analysis/1050/why-we-need-collective-redress-data-protection**

Collective Redress under GDPR

Example: The need for a form of collective redress mechanism to empower civil society to take action is recognised in Article 80(2) of GDPR. Article 80(2) provides for the ability of a "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.[19]

In summary:

Regulators should have the power to receive and act upon complaints by individuals and organisations denouncing abuse of personal data in the context of elections and political campaigns;

Regulators should have the authority to recommend and/or implement reforms when complaints reveal systemic problems;

Individuals and organisations should also have the right to seek judicial remedies for alleged violations of data protection during elections, whether directly or by appealing the decisions of regulatory bodies – and should not face prohibitive costs consequences in doing so.

[19] EDPS, Civil society are natural allies of the data protection authorities, May 2018: **https://edps.europa.eu/press-publications/press-news/blog/civil-society-organisations-natural-allies-data-protection_en**.

2. Meaningful Sanctions

Regulators need the power to impose sanctions that genuinely deter breaches of the law. This is much needed in both data protection law (some steps have been made in the GDPR, for instance, by including fines of up to €20 million or 4% of a company’s total global annual turnover) and electoral laws.

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

Regulators must have timely and effective investigative powers, including the ability to audit, investigate and to sanction and prohibit infringing behaviour. Where necessary, regulators should also have relevant prosecution powers. The threat of potential enforcement action should act as an effective deterrent rather than part of the cost of “business as normal” of a successful campaign.

D. THE GAPS

Legal Frameworks

Data protection and electoral law are by no means the only relevant legal frameworks for the regulation of political campaigning. There are many others that will be relevant and come into play – the details of which will vary from jurisdiction to jurisdiction. Examples include: telemarketing and anti-spam rules, laws that protect the confidentiality of communications (for example, the ePrivacy framework in the EU), competition law, cybersecurity rules, broadcasting and media regulations, and advertising laws (although these often exempt political advertising).

It is outside the scope of these recommendations to consider each of these. However, it is important to note that in response to the rise of digital campaigning there are increasingly initiatives around the world to introduce specific regulation, particularly when it comes to digital political advertising.[20]

Further regulation?

Whether further regulation is necessary depends on the answers to multiple questions, including whether existing frameworks (if updated and enforced, in particular as set out above in relation to data protection and electoral law) provide sufficient safeguards to regulate political campaigning.

[20] For example, the Elections Modernisation Act 2018 in Canada: **https://laws-lois.justice.gc.ca/eng/annualstatutes/2018_31/page-1.html**; in France Art. L. 163-1 of the Electoral Code introduced in late 2018 requires specific information about data use to be made available: **https://www.legifrance.gouv.fr/affichCode.do;jsessionid=83B80D3E0519E7B3D5A8AE2FC6D5D282.tplgfr42s_1?idSectionTA=LEGISCTA000006148468&cidTexte=LEGITEXT000006070239&dateTexte=20200603**. Further examples are discussed in Dobber, T. and Ó Fathaigh, R. and Zuiderveen Borgesius, F.J., "The regulation of online political micro-targeting in Europe", (2019) *Internet Policy Review* 8(4): **https://policyreview.info/articles/analysis/regulation-online-political-micro-targeting-europe**

Trends in digital political campaigning that raise such questions of sufficiency and require further consideration are political micro-targeting, the use of influencers for advertising[21], and the orchestration of organic content for campaigns. It is also clear that the underlying political industry complex – a manifold, opaque, shifting ecosystem that varies around the world – needs to be thoroughly scrutinised and held to account.

Full consideration is outside the scope of this paper, however, each of these activities may invoke aspects of the legal frameworks already highlighted. It is also important to note that as with any regulation, it is important to consider how to balance the need to be technology neutral (and thus "future proof" the framework) with the need to be sufficiently precise in order to ensure the law is clear and addresses the problem it is intended to.

In relation to political micro-targeting, we consider that a well implemented and strongly enforced data protection law already puts significant limits on micro-targeting (as set out in detail in the discussion of profiling and micro-targeting above). This should be the first priority.

Thereafter, questions remain as to whether we need more specific rules for micro-targeting, for example:

- Should there be limits during certain periods, such as in the three months prior to an election?
- Should there be limits on the targeting criteria that can be used by both campaigns and on the platforms distributing this content (for example, in some contexts targeting criteria have been limited to age, gender and postcode)?
- Should certain tools be unavailable (such as lookalike audiences) or certain practices prohibited, such as psychographic profiling?
- Do we need new mechanisms to enforce accountability from all actors, from campaigns to platforms?

[21] PI, Influence ads transparency on social media, December 2019: **https://privacyinternational.org/node/3297**

II. POLITICAL PARTIES AND POLITICAL CAMPAIGN GROUPS

This section seeks to complement the above, with specific recommendations (some of which may already be legal requirements) to political parties and campaign groups as to how to avoid data exploitation.

A. COMPLY WITH DATA PROTECTION AND ELECTORAL LAW

Political parties and campaign groups must fully comply with data protection and campaigning/ electoral laws, be accountable for all the work they do both directly and indirectly, and subject that work to close public supervision.

They must ensure that the use of data in techniques such as profiling and targeting (by them and those with whom they work) complies with all the requirements of data protection law, including principles such as transparency, fairness, purpose limitation, the requirement to have a legal basis, rights such as the right to information, and obligations such as conducting a data protection impact assessment and applying due diligence to ensure those that third parties they work with comply with the law.

B. TRANSPARENCY

In addition to the general transparency measures described above that apply to all actors in the system, political parties should also as a minimum:

- Be transparent about their data processing activities, including publicly identifying the mechanisms they use to engage with voters (e.g. social media, websites, direct messaging).
- Be transparent about how they collect people's data, what data they collect, the sources of it and how they use it.
- Adopt and publish data protection policies.
- Carry out and publish data protection audits and impact assessments.
- Specify their legal basis for each use of personal data (including any sensitive data such as that revealing political opinions).
- Be transparent as to the companies they 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 the campaign tools/ software they are using – both in-house and external.
- Make publicly available 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.
- Be transparent on political ads and messaging, ensuring that the public can easily recognise political messages and communications and the organisation behind them, and that this information is also available in an accessible online database. Make available information on any targeting criteria used in the dissemination of such political messages.
- Ensure all online and offline advertisements are publicly available and submitted to the relevant authority.

- Publish a complete, easily accessible and understandable list of any campaign groups that have financial or informal collaborative campaigning relationships with them, including all third parties and joint campaigners.
- Facilitate the exercise of data rights by individuals, including by providing information about how their data is processed and providing timely access to it.

C. LIMIT USE OF DATA FROM THIRD PARTIES

In order to gain access to increasing amounts of data on voters, political parties or the companies they work with often buy data from third party sources. This data is then used for profiling and targeting of voters.

Ultimately, given the problematic nature of the way much data is gathered and used for profiling, campaigns cannot comply with relevant legal requirements without reconsidering the procurement of data from these companies. Indeed, the UK data protection authority, the Information Commissioner's Office, called for such an 'ethical pause' in July 2018, before there is greater expansion of the use of new technology in political campaigning.[22]

[22] UK Information Commissioner, Democracy Disrupted? Personal information and political influence, July 2018: **https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf**

III. COMPANIES

Again, this section aims to complement the requirements of strong legislation, namely data protection and electoral law, by providing specific recommendations (some of which may already be legal requirements) for the range of companies that play a role in the digital campaigning ecosystem.

These include:

- Data brokers
- Analytics companies
- Campaigning platforms
- Companies that facilitate the behavioural and micro-targeted advertising system (AdTech)
- Online platforms providing advertising
- Social media and messaging applications

A. GENERAL

1. Comply with the law

All companies must fully comply with their legal obligations. This includes data protection and may also include campaigning/ electoral laws. Companies must ensure that their activities, whether data gathering, using data for profiling and targeting, or building tools that facilitate these techniques all comply with data protection laws. They must be accountable for this and their role in political campaigns. Companies should also respect human rights. A starting point for doing the latter would be to abide by the UN Guiding Principles on Business and Human Rights.

2. Voluntary measures/self-regulation not a sufficient response

Certain companies have proposed and implemented voluntary measures on political campaigning issues and transparency in advertising in some parts of the world – these responses have been patchy and inadequate. The issues at stake are too important to be left to the discretion of a handful of companies, which is no substitute for a democratic response. It is not however, an excuse to not be proactive and respond to concerns.

3. Cross-jurisdictional implementation

Industry should implement best practices across all jurisdictions, not only in those that have legislated or enforced such practices.

B. TRANSPARENCY

1. General

Transparency should be provided by companies involved in all stages of political campaigning – whether in data gathering, profiling, the development of campaign tools or the deployment or facilitation of targeting.

As a starting point, all companies should comply with the transparency requirements of data protection law. Below, we provide suggestions for specific information that different types of companies should be providing, but that is often lacking, making it hard to get a meaningful understanding of how data is being used in political campaigns. They are my no means exhaustive.

More transparency is required at every stage from data gathering to profiling to targeting, including with regard to:

- data sources
- data collection methods
- actual data collected
- if, by whom and for what purpose profiling is used
- the detail of profiling practices
- the categories of data that may be inferred and on what basis
- segments/ attributes with which someone may be linked and why
- how these profiles are intended to be used/ have been used
- if these profiles have been shared, with whom and for what purpose
- the potential consequences of this profiling
- the full targeting criteria available

- what categories were used to target a particular message
- targeting techniques
- how custom and lookalike audiences work
- who is behind ads i.e. who sponsors, who creates, who uploads
- criteria used to determine what and how content is delivered

Given the difficulties in defining what constitutes political advertising and the many actors involved, effective ads transparency must go beyond "political ads" and scrutiny must not be limited to one particular platform. Solutions must enable meaningful transparency for users as well as effective scrutiny by researchers and civil society.

2. Platforms

Platforms that facilitate targeted political messaging should as a minimum:

- Be transparent about how political campaigns can use their platform and whether there are any restrictions in place.
- Be transparent about any political campaigns they are working with, including directly, such as by embedding staff into a campaign.
- Be transparent about any policies in relation to political or issue ads and communications, as well as how those policies are monitored and enforced.
- Be transparent as to how they define/ or what criteria or conditions they use to classify political or issue-based ads and the basis for this.
- Be transparent in relation to any specific measures or steps being taken in specific contexts, such as an upcoming election or referendum, as well as to who, and how, any concerns may be raised directly.
- Be transparent to users about how ads are targeted, this includes insight into: what data was used to target the ad, including the source of that

data; the target and audience of the advertiser; who uploaded the ad; who sponsored the ad and paid for it; if and how profiling was used to target the ad; what data was used in any custom audience or equivalent, and whether the data was used to create a 'lookalike' audience or equivalent and/ or whether the ad is being shown an ad as part of a 'lookalike' audience, as well as the targeting information and criteria used by the platform in displaying any such ad; and information on how to complain about an ad, use data rights in relation to an ad and block an ad.

- Ensure that ads, including political and issue ads, are publicly accessible at all times through full advertising archives. The data in the archives should be relevant for statistical analysis, freely accessible, searchable and machine readable through an API that allows large scale analysis. This should be available for users across the global, but where there are relevant national election rules these can act as a baseline. The archives should include information about:
    - data sources / collection;
    - data collection methods;
    - the targeting criteria;
    - intended v actual audience;
    - whether a message is being targeted using a custom or lookalike audience or equivalent;
    - how much was spent on an ad;
    - how long an ad ran for;
    - who uploaded the ad;
    - who sponsored the ad and paid for it; and
    - 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.

- Be transparent about their profiling practices, including how profiling is used to facilitate the personalisation and targeting of what people see. This is of heightened importance during an electoral period and does not just apply to overtly political content.
- Be transparent about steps being taken to ensure sponsored content or other forms of alternative advertising occurring on their platform are included within any transparency efforts.
- Be transparent as to reporting mechanisms and provide information on the number of complaints received and how they were resolved.
- Be transparent as to the steps they have taken to comply with data protection obligations, including due diligence in relation to data sources used for targeting and the legal basis for this; the requirement to implement data protection by design and by default; the requirement to carry out data protection impact assessments for intrusive and large scale processing; and how they facilitate the exercise of data rights, including the right to access or the right to object.

3. Data brokers, AdTech and the wider 'Influence Industry'

When we refer to data brokers and AdTech companies, we are attempting to encompass a vast and complex ecosystem of companies that play a range of roles from gathering data from our devices through various tracking techniques (from cookies, to pixels, to fingerprinting), to the combination, sourcing and segmenting of data into detailed profiles, to the development of campaign tools, to the targeting of content at us through real time bidding. All of which are techniques now used in political campaigning. There are companies in this sector dedicated specifically to political campaigns. There are also companies that offer a broad range of services, primarily for commercial advertising, but also in political contexts. Even where companies do not explicitly offer services to political campaigns, they may be used by such. What all these companies have in common is that they profit from people's data, or the development of tools to facilitate the exploitation of people' data, for the purpose of seeking to influence behaviour – whether that be commercial or political.

Given the range and complexity of the actors involved, it can be hard to make general recommendations. Indeed, we question whether these companies can ever comply with the legal standards set out above. Strong consideration should be given to limiting their involvement in political campaigns.

However, transparency is a key starting point, given that what characterises the majority of these actors – most of which are not known to the public – is their opacity. They should, as a minimum:

- Be transparent about how they comply with their legal obligations, including under data protection, such as the obligation to have a clear lawful basis for their activities, to disclose what data they have, where they source this data, what they do with it, who they share it with and for what purposes, as well as their obligation to implement data protection by design and by default.
- Publish the names of any clients involved in political campaigning and what services they provide to them, including any data provided or data processing activity (such as, for example, the provision of a tool used in campaigning) and provide these to relevant regulators to ensure they have the full picture.
- Carry out and publish data protection impact assessments in relation to any work related to political campaigning.
- Be transparent about any and all profiling activities.
- Be transparent about how they ensure individuals whose data is processed by them or their clients are provided with the information they are entitled to, as well as information about how those individuals can exercise their data rights.

FURTHER INFORMATION

Selection of PI resources and advocacy on the use of data in the political context (2018 – 2020)

- Dec 2018, PI Response to ICO call for views on Code of practice for data in political campaigns: **https://privacyinternational.org/node/2838**

- March 2019, PI submission to the Interamerican Commission of Human Rights on Disinformation in Electoral Contexts: **https://privacyinternational.org/advocacy/2851/disinformation-electoral-contexts-engagement-interamerican-commission-human-rights**

- April 2019, PI, 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**

- May 2019, PI, Data exploitation & Democratic Societies: **https://privacyinternational.org/long-read/2850/data-exploitation-and-democratic-societies**

- June 2019, PI response to the Centre for Data Ethics and Innovation's Review of Online Targeting: **https://privacyinternational.org/advocacy/3092/pis-submission-centre-data-ethics-and-innovations-review-online**

- July 2019, PI, Election Cycle: Technology, data and elections – checklist: **https://privacyinternational.org/advocacy/3093/technology-data-and-elections-checklist-election-cycle**

- July 2019, PI submission to the UK APPG on Electoral Campaigning Transparency: **https://privacyinternational.org/node/3104**

- August 2019, PI letter with ADC *et al.* to Facebook, Google and Twitter re political advertising in Latin America and the Caribbean: **https://privacyinternational.org/node/3183**

- Sept 2019, PI submission to the House of Lords Committee on Democracy and Digital Technologies: **https://privacyinternational.org/advocacy/3239/pi-submission-house-lords-committee-democracy-and-digital-technologies**

- Oct 2019, PI, Social media companies have failed to provide adequate advertising transparency to users globally: **https://privacyinternational.org/node/3244**

- Oct 2019, PI response to the ICO's draft Code of Practice for Data in Political Campaigns: **https://privacyinternational.org/advocacy/3267/submission-ico-code-practice-use-personal-data-political-campaigning**

- Dec 2019, PI joins call for updated electoral regulation following 2019 UK General Election: **https://privacyinternational.org/news-analysis/3311/pi-joins-call-updated-electoral-regulation-following-2019-uk-general-election**

- Feb 2020, PI, Questions that should be asked and answered on the use of personal data in elections: **https://privacyinternational.org/node/3359**

- March 2020, ICO consultation on Direct Marketing Code of Practice – PI response: **https://privacyinternational.org/node/3398**

Selection of guidance and opinions by data protection authorities on use of data in the political context

- 2005 ICCDPC Resolution on the Use of Personal Data for Political Communication: **http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Personal-Data-for-Polictical-Communication.pdf**
- March 2014, Italian Data Protection Authority (Garante), Rules on processing of personal data by political parties: **http://www.garanteprivacy.it/web/guest/home/docweb/-/docwebdisplay/docweb/3013267**
- November 2016, French Data Protection Authority (CNIL) guidelines to its 2012 recommendations on political communication: **https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux**
  Further guidance here: **https://www.cnil.fr/en/tag/elections**
- March 2018, EDPS, Opinion 2/2018 EDPS Opinion on online manipulation and personal data: **https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf**
- July 2018, ICO Democracy Disrupted report: **https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf**
- July 2018, ICO updates to DCMS Committee: **https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf**; Nov 2018, ICO Guidance on political campaigning: **https://ico.org.uk/media/1589/promotion_of_a_political_party.pdf;** and draft code of practice for the use of personal data in political campaigning: **https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf**
- September 2019, European Commission guidance on the application of Union data protection law in the electoral context: **https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf**
- March 2019, European Data Protection Board (EDPB), Statement 2/2019 on the use of personal data in the course of political campaigns: **https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf**
- December 2019, Agencia Española de Protección de Datos (AEPD), Spain, Opinion on processing of personal data by political parties: **https://www.aepd.es/sites/default/files/2019-09/2018-0181-tratamiento-datos-opiniones-politicas-por-partidos-polticos.pdf**
- March 2019, AEPD, Circular on processing of political personal data, March 2019: **https://www.boe.es/boe/dias/2019/03/11/pdfs/BOE-A-2019-3423.pdf**
- May 2019, Spanish Constitutional Court decision striking down exemption for political parties, Judgment (in Spanish): **https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/2019-1405STC.pdf**; and press release in English: **https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_076/Press%20Release%20No.%2076.2019.pdf**
- October 2019, Colin Bennett, Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities, ICDPPC 2019: **https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf**
- October 2019, International Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising Other Fundamental Rights: **http://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf**

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org