Public Consultation: **Disinformation in electoral contexts**

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR/RFOE), OAS Department of Electoral Cooperation and Observation (DECO) and the Department of International Law (DIL) - Organisation of American States

Privacy International's response

March 2019

PRIVACY INTERNATIONAL

1. About Privacy International

Privacy International is a registered charity based in London that works at the intersection of modern technologies and rights. Privacy International works with our partners around the world, including in OAS countries[1], to fight for the right to privacy for people everywhere.

Privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. In order for individuals to fully participate in the modern world, developments in law and technologies must strengthen and not undermine the ability to freely enjoy this right.

Privacy International has many years of experience challenging state and corporate surveillance and data exploitation. A core focus of Privacy International's work is tackling digital threats to democracy, looking at the exploitation of data in the electoral cycle, with a particular focus on political campaigns and advertisement. As set out in this response these topics are highly relevant to the consultation topic of "Disinformation in electoral contexts".

Contact: Ailidh Callander, Legal Officer ailidh@privacyinternational.org

2. Executive Summary

Privacy International welcomes the opportunity to respond to this timely consultation on "Disinformation in electoral contexts" by the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, OAS Department of Electoral Cooperation and Observation and the Department of International Law. The issues which this public consultation seeks to inform require a joined up, multi-institutional approach and thus it is a positive step that these factions of the OAS are working together to consult.

[1] https://privacyinternational.org/location/latin-america

To consider the issue of 'disinformation in electoral contexts' it is essential to look at the use of data. If we think of disinformation as the 'front end', then we recognise that data is the 'back end' that feeds into and facilitates many of the practices that raise concerns.

Privacy International's submission therefore takes the form of a general comment around data in political campaigning, and of the three topics flagged in the call for views, focusses on that of "possible actions and actors involved".

We have also included as a final section a list of studies and reports that may useful in the consideration of this topic.

This submission is not exhaustive of the issues nor Privacy International's position and we look forward to engaging further with the OAS on this topic.

3. The importance of data

To consider the issue of 'disinformation in electoral contexts' it is essential to look at the use of data by the multiplicity of actors in the electoral and political campaigning context. If we think of disinformation as the 'front end', then we recognise that data is the valuable 'back end' that feeds into and facilitates many of the practices that we are concerned about.

Political campaigns around the world have turned into sophisticated data operations. They rely on data to facilitate a number of decisions: where to hold rallies, which States or constituencies to focus resources on, which campaign messages to focus on in which area, and who and how to target and with what messages.

There are many different issues to unpack in this topic, but Privacy International is particularly concerned by the data ecosystem that drives voter profiling and targeted messages, often known as micro-targeting, that accompanies modern political campaigning globally.

Targeting in any form is reliant on data. The sources of such data are multiple. Political parties and campaigns gain access to commercial data, through data brokers, platforms, political data consultants, to name a few. They also collect and generate their own data of members and also

through canvassing and other activities such as apps, online tracking, surveys and competitions. In many countries political parties are also provided with access to the electoral roll/ voter registration records.

Data can be exploited through a range of mediums and platforms where messages can be disseminated in a targeted manner, this ranges from the use of text messages (SMS), [2] to calls, to messaging apps (e.g. Whatsapp), to search results (e.g. through AdWords), to campaign apps, ad supported platforms (e.g. Google, Facebook, Twitter, YouTube, Instagram) and publishers. Any platform that aims to facilitate targeted messaging, even if it is not their main objective or core business can be eventually used for microtargeted campaigns.

This is in large part driven and facilitated by the targeted ad-supported internet, made up of thousands of companies that track and profile individuals 24 hours a day, not just during election periods.

This can be tapped into at any moment for political purposes. As Alexander Nix CEO of the now infamous company Cambridge Analytica is reported as having said "What we are doing is no different from what the advertising industry at large is doing across the commercial space". [3] This does not legitimise these practices either in the commercial sphere and particularly not in the political arena.

While data driven political campaigns are not new, the granularity of data available, the scale and the potential power to sway or suppress voters through that data is. The way in which data is used in modern political campaigning is highly privacy invasive, raises important security questions, and has the potential to undermine faith in the democratic process, including in relation to transparency, fairness and accountability.

It is well known that Facebook and Google's business models are so lucrative because of the ability to offer targeted advertising, based on user information like age, location, interests, and even the use of 'lookalike' or similar audiences. This has proved so appealing that political parties want in - so in the same way that online advertising targets people based on interests,

[2] Investigating privacy implications of biometric voter registration in Kenya's 2017 election process. Robert Muthuri, University of Strathmore. Available in https://privacyinternational.org/sites/default/files/2018-06/Biometric%20Technology-Elections-Privacy.pdf

[3] Evidence by Alexander Nix, former CEO Cambridge Analytica to UK Parliament 27 February 2018, available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/79388.pdf

personality and mood to ultimately sell products, political parties try to persuade you to buy what they are selling come election time.

The platforms want political actors in on the 'game' too and actively market and showcase their tools and services in the political sphere.[4] They are only belatedly waking up to the potential consequences, in large part due to journalists, civil society, public, academic, regulatory and parliamentary scrutiny and pressure.

There is a complex and opaque corporate ecosystem behind targeted online political advertising. This is not just the Facebooks, Google and Twitter - data brokers and data analytics companies should all be part of this conversation as well as the wider ad tech ecosystem.[5]

As well as using the platforms directly, data analytics and digital media firms are employed directly by political parties to run online campaigns. The details are often unclear- exactly who these companies work for, what they do and how they do it is often a guarded secret.
What is clear is that there are thousands of companies whose business model it is to exploit people's data in such a way that intimate personal details about a person's beliefs, habits, and behaviour can be better understood and used for the purpose of allowing political parties to target these individuals with political messages. Anyone with sufficient resources can take advantage of these tools and troves of data to seek to push their own political agenda.

Those companies can operate globally (sometimes through subsidiaries or representatives), or locally, with very low levels of transparency and even lesser levels of accountability.

Privacy International started looking at this issue back in 2017 investigating the involvement of Cambridge Analytica and US far right media consultancy – Harris Media – in the Kenyan Elections.[6] Civil society, academics and journalists around the world are continuing to document

[4] For example, Google's role in the Macri campaign in elections in Argentina https://ourdataourselves.tacticaltech.org/posts/overview-argentina/ or Facebook and data broker's Acxiom's role in the Conservative party campaign in the UK https://www.facebook.com/business/success/conservative-party#u_0_0

[5] In November 2018, Privacy International filed complaints against data brokers, credit reference agencies and AdTech companies with data protection authorities in the UK, Ireland and France. More information here: https://privacyinternational.org/press-release/2424/privacy-international-files-complaints-against-seven-companies-wide-scale-and

[6] https://privacyinternational.org/feature/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack

the misuse of data in elections, this includes in OAS countries, for example in Argentina,[7] Chile,[8] Mexico,[9] Brazil,[10]Colombia[11] and the USA.[12]

Often the laws and regulatory mechanisms are insufficient or there is an enforcement gap. However, to begin to tackle this data exploitation it is important to look at relevant legal frameworks – human rights, data protection and electoral law. These frameworks should be in place, strengthened and implemented. They also need well resourced, independent regulators and courts to enforce them.

All of these issues are intrinsically related to the power of certain actors and the opaque nature of their practices, therefore other legal tools such as competition or antitrust laws may also be relevant.

Certain companies have proposed and implemented voluntary measures in some parts of the world, however, the issues at stake are too important to be left to the discretion of a handful of companies and no substitute for a democratic response.

4. Actions and actors involved

4.1. Actions

In considering the use of data in the back end of disinformation in the electoral context and possible actions, it is important to acknowledge that (i) data exploitation in political campaigning is not limited to the electoral period and (ii) there are a number of actors involved using different tools and techniques to exploit data.

Political campaigning is not limited to the strict electoral period and thus neither is the exploitation of data and the disinformation which it can feed. The collection, generation and

[7] Report by Asociación por los Derechos Civiles (ADC), Argentina: https://adcdigital.org.ar/wp-content/uploads/2018/07/ADC-microtargeting-PRO-Cambiemos.pdf
[8] Report by Datos Protegidos, Chile https://datosprotegidos.org/wp-content/uploads/2018/09/Informe-datos-electorales.pdf
[9] Report by 'Son Tus Datos, Articulo 12, México https://sontusdatos.org/wp-content/uploads/2018/07/180629-a12-datos_personales_e_influencia_politica-vf.pdf
[10] Report by Coding Rights, Brazil https://www.codingrights.org/wp-content/uploads/2018/11/Report_DataElections_PT_EN.pdf
[11] Report by Karisma, Colombia https://karisma.org.co/descargar/elecciones-y-datos-personales-un-estudio-de-las-elecciones-legislativas-de-2018/
[12] Report by Jeff Chester and Kathryn C. Montgomery, USA https://ourdataourselves.tacticaltech.org/media/ttc-influence-industry-usa.pdf

use of data which may be used in political campaigning happens at all times, and not just around elections.

For example, data can be used for political campaigning and elections outside the electoral context (e.g. UAE and Saudi Arabia's use of ads/social media campaigns to seek to influence US policy on Qatar[13] or the use of spyware on supporters of a sugar tax in Mexico[14]).

There might not be obvious links between the way the data is used politically for example in an effort to influence or create division, and a political party manifesto commitment or support or opposition in a referendum. As an example, a report prepared for the US Senate on Russian disinformation provides details on how people in the US were categorised into key interest groups for targeted messaging, including through Internet Research Agency controlled Facebook pages such as "Being Patriotic", "Heart of Texas", "Blacktivist" and "Army of Jesus". Furthermore "[the IRA] operated 133 accounts on Instagram, a photo-sharing subsidiary of Facebook, that focused mainly on race, ethnicity or other forms of personal identity. The most successful Instagram posts targeted African American cultural issues and black pride and were not explicitly political."[15]

Political parties are just one of many actors involved. There are many other actors that play a role (whether intentional or unintentional) in political campaigning (including through influencing and nudging) but do not have a direct relationship with/are not affiliated with a particular party or candidate. Even the targeted nudge to vote can have significant impacts in an electoral process.[16]

Therefore, in examining these issues, it is important to not only focus on the official election or campaign period or solely on the registered political parties or official candidates as this risks missing a significant proportion on actions and actors that may seek to directly influence democracy and public discourse[17].

4.2. Actors

[13] See: https://www.pri.org/stories/2018-07-24/how-diplomatic-crisis-among-gulf-nations-led-fake-news-campaign-united-states

[14] See: https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax- advocates.html)

[15] https://www.washingtonpost.com/technology/2018/12/16/new-report-russian- disinformation-prepared-senate-shows-operations-scale-sweep/?utm_term=.12b0a47d7c1f

[16] See: https://www.theguardian.com/technology/2018/apr/15/facebook-says-it-voter-button-is-good-for-turn-but-should-the-tech-giant-be-nudging-us-at-all

[17] See: https://www.politico.eu/article/britain-nationalist-dark-web-populism-tommy-robinson

In considering the actors involved it important to consider the wide spectrum of actors not just political parties, but those whose tools, goods and services they use – this includes the overlap with the actors in the commercial advertising sector (which is dominate by giants such as Facebook and Google but made up on hundreds of other data companies) and those that have honed down these practices for the political sphere.

There are many ways to divide up the Actors involved, and these are just a few:

- Political Parties
- Political Campaign Groups
- Data Brokers
- Analytical companies
- Campaigning platforms
- Companies that facilitate the behavioural and micro-targeted advertising system (AdTech)
- Online platforms providing advertising
- Social Media and Messaging applications

To get an understanding of the data broker and data analytics companies involved in political campaigning, we recommend consideration of the research by Berlin based NGO Tactical Tech, who have collated information on hundreds of companies operating in this sphere. Tactical Tech divided the organisations' roles into: Data as influence: Campaigning; Data as influence: Communications; Data as an asset; and Data as intelligence. Many of the companies fall into multiple categories.[18] Including data brokers and advertising companies.

Concerns around data brokers, and the online advertising ecosystem are reflected in investigations and actions by civil society. For example, in November 2018, Privacy International called on the ICO, together with the Irish and French data protection authorities, to investigate seven data broker and advertising technology companies, that are illustrative of more systemic problems.[19] Whilst these complaints do not focus on political campaigning, they focus on actors that rely, thrive and profit from personal data. As already noted, the techniques and data intensive ecosystem used in commercial advertising are also deployed in the political context

[18] https://ourdataourselves.tacticaltech.org/posts/whos-working-for-vote and https://ourdataourselves.tacticaltech.org/media/data-companies-and-digital-consultants-long- list_updated-28th-Nov-2018.pdf

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

with a number of these actors Privacy International complained about, advertising specific offerings for the political context e.g. Oracle[20] and Experian in the US, and Experian in the Brazilian elections.[21]

Advertising and political campaigning have become intertwined and inextricable. As the founder of one political campaigning company put it: "There are tons and tons of consumer data on the ad exchanges that we built [...] you have registrations that are publicly available information. You can take those voter rolls and match those to our online profiles and serve those people ads individually online."[22]

5. Key legal frameworks to consider

As noted above, in order to address the exploitation of data that in turn feeds disinformation, consideration is needed of human rights mechanisms, including those around the right to privacy, the right to freedom of expression, the right to political participation as well as other safeguards that might be relevant, such as the provisions of the Inter-American Democratic Charter. The human rights framework must be supplemented by specific laws regulating the use of data and the electoral environment. Other legislative frameworks may also be of relevance such as competition law and advertising law.

5.1. Data protection law in an international context

The right to individual privacy is an increasingly important aspect of international law. The right is enshrined in the foundational documents of the international human rights system, and it has only become more detailed and prominent in the digital age.

International human rights mechanisms have been clear that the unauthorized processing of personal data infringes on the right to privacy and have emphasized the importance of data protection laws in enforcing that basic right.[23] Over 120 countries around the world have now enacted data protection legislation of varying strengths.

---

[20] See: http://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf

[21] https://www.experian.co.uk/assets/marketing-services/brochures/experian-marketing-services- brochure.pdf ; see Audience IQ which provides political segments https://www.experian.com/assets/marketing-services/product-sheets/das-political-data-sheet.pdf; as explained here: https://ourdataourselves.tacticaltech.org/posts/psychometric-profiling/ and their role in the 2018 election in Brazil https://www.codingrights.org/wp-content/uploads/2018/11/Report_DataElections_PT_EN.pdf

[22] See: https://ourdataourselves.tacticaltech.org/posts/the-new-disruptors

[23] In 2018, the UN High Commissioner for Human Rights report on the right to privacy in a digital age recognised that laws setting standards for the processing of personal information by both States and private actors are a cornerstone of State privacy protection, available at: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/39/29

However, when considering the effectiveness of these laws, it is important that they are comprehensive in their application, with a resourced, independent regulator; and with political parties or groups do not benefit from exemptions or loopholes.
Most data protection laws around the world give special protection to personal data revealing political opinions, in recognition of the sensitivity of this data and significance of the consequences of its use.

As more and more data is generated about individuals every day the more that can be revealed about individuals' political opinions even where such opinions are not explicit. Therefore, a key aspect that data protection law should deal with is profiling.
Data can be used to develop profiles of both individuals and groups and data inferred about individuals must be considered personal data under the law.

Data that feeds into such profiles is bought, amassed and shared from and between multiple actors,[24] without individuals having ever known they were profiled. Profiles can be cross-correlated and used to infer data not just about an individual but others 'like them', for example through 'lookalike audiences'. Furthermore, data brokers and ad tech companies often offer probabilistic solutions i.e. they will establish "a match between sets of data leveraging inferred, modelled or proxy assumptions".[25] This can happen not only in the commercial sphere but in the political and consideration must be given to how the protections that extend to explicitly political data extend to such profiling practices. This includes where profiles are developed based on aggregated data but then associated with individuals and or where tools enable political actors to reach individuals based on certain data points without actually having their data (e.g. through retargeting).

5.2. Electoral Laws

Electoral laws must be fit for purpose in a digital campaign environment. By electoral laws we mean not only the laws regulating the running of the elections but also aspects such as voter registration, access to voter records, registration of political parties and candidates, campaigning including financing, transparency, oversight, and the media. Too often these laws

[24] See: https://privacyinternational.org/feature/1721/snapshot-corporate-profiling and https://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad.
[25] Winterberry Group Report: "Know Your Audience: The Evolution of Identity in a Consumer-Centric Marketplace", August 2018 https://www.winterberrygroup.com/our-insights/know-your-audience-evolution-identity-consumer-centric-marketplace

have not been updated for the digital age, for example, the same safeguards that apply to print and broadcast in elections do not even apply and in a digital environment and only the voter, campaigners and platform know who has been targeted with which messages.

Among other matters, if electoral law is to be effective in regulating digital campaigning, seeking to ensure transparency, fairness and accountability in the electoral process, review and reform may be needed. Consideration includes transparency of campaign financing and advertising, spending caps relating to campaigning, timing and granularity of reporting requirements as well as the powers and sanctions of regulators. In the UK, the Electoral Commission issued a set of recommendations on this subject. [26]

6. Recommendations

In terms of next steps, we propose the adoption of the following urgent measures to address these issues:

- Legal frameworks need to be examined to make sure that they account for the issues described in this submission. In particular, data protection and electoral laws needs to be closely examined in order to address the use of data in electoral campaigns from a comprehensive perspective. Where these frameworks fall short, they should be amended and enhanced.

- Regulators must be empowered to provide clear guidance, take action and enforce the law, having the ability to conduct their work without external pressure and with the ability to request information from all involved parties: political parties, campaign groups, private actors, and other government actors involved in the electoral cycle. Regulators must be given the necessary resources (financial and capacity) to take such action.

- 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.

[26] Available in: https://www.electoralcommission.org.uk/__data/assets/pdf_file/0010/244594/Digital-campaigning-improving-transparency-for-voters.pdf

- Industry actors need to be transparent and accountable with regard to the services and products they offer to political parties around the world, and the methods used to obtain and process personal data.

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

- All parties involved in the electoral cycle, including national electoral commissions and electoral monitoring bodies, need to receive proper capacitation on these issues according to their roles, including the type of technologies and methods deployed for campaigning, applicable privacy and electoral law, and on good practices of how to exercise their powers.

- Support is needed for civil society and public interest actors seeking to scrutinise, monitor and expose abuse of data in the electoral context.

7. Additional resources

A non-exhaustive selection: -

Civil Society

- Privacy International – data and elections work: https://privacyinternational.org/topics/data-and-elections
- Tactical tech – data and politics project: https://ourdataourselves.tacticaltech.org/projects/data-and-politics/ including personal data" political persuasion – Inside the Influence Industry. How it works (March 2019) https://tacticaltech.org/media/Personal-Data-Political-Persuasion-How-it-works.pdf
- Constitution Society Report https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey- Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf
- Tracking tools: Whotargetsme: https://whotargets.me/en/ ; ProPublica: https://projects.propublica.org/facebook-ads/?lang=en-US Facebooktrackingexposed: https://facebook.tracking.exposed

Parliaments

- 'International Grand Committee 'Principles of the Law Governing the Internet' https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/declaration-internet-17-19/
- EU action plan, including Code of Practice on Online Disinformation and roadmap for implementation: http://europa.eu/rapid/press-release_IP-18-6647_en.htm
- European Parliament decision on the use of Facebook users' data by Cambridge Analytica and the impact on data protection: http://www.europarl.europa.eu/doceo/document/B-8-2018-0480_EN.html?redirect
- UK Digital, Culture, Media and Sport Committee
    - Disinformation and 'fake news Interim Report – 29 July 2018 https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf
    - Disinformation and 'fake news Interim Report – 18 February 2018 https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

- Canada, the Standing Committee on Access to Information, Privacy and Ethics report: https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf

Data Protection Authorities

- European Data Protection Board: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf
- European Data Protection Supervisor: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
- UK: https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/
- Spain: https://www.aepd.es/prensa/2018-12-19.html
- Italy: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9081475