February 2021

Privacy International's submission on 'disinformation'

Privacy International (PI)[1] welcomes the call for submissions by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to inform the Special Rapporteur's report on 'disinformation' and freedom of expression.[2]

The issues highlighted in the call for submissions are ones that PI with its global network of partners[3] has been investigating as part of its work on the use of personal data, and the hidden ecosystem involved, in the online political campaigning context. This submission is intended to serve as a global overview of the factors that PI has identified as playing a significant role in facilitating the spread of 'misinformation'. The focus of PI's work has been on the online campaigning context. However, we expect that many of the observations below could also be relevant for other contexts as well.

In particular the following submission highlights:

- The role played by online platforms in facilitating the spread of misinformation by political actors through insufficient and limited transparency on political advertising; and
- The need for electoral regulators to be able to enforce higher transparency requirements in the online campaigning sphere.

1 Privacy International (PI) is a London based registered charity that works globally at the intersection of modern technologies and rights. We challenge overreaching state and corporate surveillance, so that people everywhere can have greater security and freedom through greater personal privacy. We are fighting for a world where technology will empower and enable us, not exploit our data for profit and power.

2 https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Report-on-disinformation.aspx

3 PI, Our Global Reach, available at: https://privacyinternational.org/where-we-work

Recommendations

PI suggests the following recommendations to be included in the Special Rapporteur's report on disinformation:

- Online platforms must ensure that they provide meaningful transparency to users in relation to the political ads that they see;
- Online platforms must ensure that the highest possible transparency standards are made available to all countries where they allow political advertising to take place, while protecting vulnerable advertisers;
- Online platforms must ensure that political ads are displayed to users on an opt-in basis;
- Governments must ensure that their national law, including electoral regulation, is fit for purpose in the age of digital campaigning;
- Data protection agencies should consider the impact of modern online campaigning techniques on data protection and privacy.

I. Disinformation, freedom of expression, privacy and data protection

While not readily apparent, there is a strong link between disinformation and the exploitation of personal data, as well as the right to freedom of expression and the right to privacy. To consider the issue of 'disinformation' 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.

This connection manifested itself clearly in the run-up to the US 2020 Presidential Election, where Latino and Black voters were disproportionately targeted with disinformation efforts aiming to suppress minority votes.[4] A 2020 investigation uncovered similar tactics having been used in the US 2016 election, with millions of African Americans being shown highly tailored advertising to deter them from voting.[5] Where a person is targeted on the basis of belonging to a minority or another group, legitimate questions arise as to how they came to be identified as such, and whether

4 NPR, *Black and Latino Voters Flooded with Disinformation in Election's Final Days*, 30 October 2020. Available at: https://www.npr.org/2020/10/30/929248146/black-and-latino-voters-flooded-with-disinformation-in-elections-final-days?t=1613141230798

5 Channel 4, *Revealed: Trump campaign strategy to deter millions of Black Americans from voting in 2016*, 28 September 2020. Available at: https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016

the data revealing their ethnicity, or any other shared characteristics, was lawfully processed by the advertiser.

Targeting in any form is reliant on personal data.[6] The sources of such data are multiple, ranging from electoral registers to commercially available sources, such as data brokers and online platforms. While data-driven political campaigns are not new, the granularity of data available, and the scale and potential power to sway or suppress voters through that data is. New online campaigning tactics documented by PI, such as micro-targeting, enable disinformation strategies to flourish and succeed.[7]

The way in which data is used in modern political campaigning is highly privacy-invasive, and raises important data protection questions.[8] To the extent that personal data is used to convey messages in support of or against a campaign, data protection concerns intersect with the exercise of freedom of expression in electoral contexts.

Data can be exploited through a range of mediums and platforms where messages can be disseminated in a targeted manner.[9] This ranges from the use of text messages (SMS), 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 can be eventually used for microtargeted campaigns, even if that is not their main objective or core business.

This data exploitation 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. The vast trove of data held by these companies can be tapped into at any moment for a range of purposes, including political campaigning.

---

6 PI, *When Your Data Becomes Political*. Available at: https://privacyinternational.org/taxonomy/term/618

7 PI, *Micro-targeting*. Available at: https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016

8 PI, *Why we're concerned about profiling and micro-targeting in elections*. Available at: https://privacyinternational.org/news-analysis/3735/why-were-concerned-about-profiling-and-micro-targeting-elections

9 PI, *Disinformation in Electoral Contexts*, Response to the consultation by OAS Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights. Available at: https://privacyinternational.org/sites/default/files/2019-04/19.03.28%20CIDH%20Consultation%20Response.pdf

II. Measures taken by digital tech companies to address misinformation

There is a complex and opaque corporate ecosystem behind targeted online political advertising. In the paragraphs that follow, we briefly reflect on the effectiveness of some of the measures taken by online platforms to target misinformation.

The implementation of ads transparency tools

In PI's view, a key avenue for digital tech companies to limit misinformation is to provide detailed information and heightened transparency standards for individual ads.[10]

Transparency is crucial to combat misinformation because it enables users to understand, contextualise, and critically assess, the ads that they see. By being able to consider the expense involved in an ad, the relevant political party or candidate behind it, and the personal data and criteria used to target them, users can better understand the advertisers' resources, campaigning strategy, data processing activities, and biases. These categories of information can play a crucial role in users' receptiveness, processing and reaction to misinformation online.

All forms of transparency should operate at two levels: first, detailed information should be immediately available to the user upon seeing a political advertisement; second, the ad itself, and related information, should be visible to users and civil society at large by way of inclusion on an online ad repository. The former enables users to exercise their judgment in relation to a specific ad; the latter enables civil society and researchers to scrutinise the wide range of ads posted by each candidate or political party on the platform, ensuring memory and accountability.

In the absence of scrutiny, political ads can contribute to democratic harms. PI's research, carried out with the Institute for Policy Research and Advocacy (ELSAM) in Indonesia, found political ads relying on stoking racial tensions and xenophobia for effectiveness. An example is provided below.

10 PI, *Why is advertising transparency important*? Available at: https://privacyinternational.org/explainer/3288/why-advertising-transparency-important



Ad seen during the 2019 Indonesian general election stating "Curtail the Foreign Labourers"

In our January 2021 report *Online political ads – a study of inequality on transparency standards*, [11] we assessed the steps taken by Facebook and Google to improve transparency in the online political campaigning context. The tools they have developed to this effect broadly fall in two categories: advertiser verification measures and inclusion of ads in an online repository. However, these tools have been implemented only in selected countries and have not been made available equally to all users.

Facebook

In countries which benefit from heightened ads transparency standard, Facebook carries out mandatory checks on political advertisers prior to them being able to post

11 PI, *Online political ads -a study of inequality on transparency standards*. Available at: https://privacyinternational.org/sites/default/files/2021-01/AdsTransparency_TOPUBLISH.pdf

political ads, and automatically includes political ads in the Ad Library (Facebook's online ad repository).

Despite Facebook's efforts in 2020 to substantially increase the number of countries where mandatory checks were available for political advertising, these countries still remain a minority. In the vast majority of countries where Facebook operates, transparency tools are available, but option: political advertisers may verify their identity and include their ads in the Ad Library, if they so choose.

PI's research reveals that "optional" transparency requirements are not sufficient.[12] In Peru, a country which did not benefit from mandatory transparency requirements before 2021, almost no candidates in the 2020 Peruvian congressional election availed themselves of Facebook's optional transparency tools. As reported by partner organisation Hiperderecho, out of 2,325 candidates who ran for Congress, only four used Facebook's optional tools to provide transparency information about their ads. [13]

Colombia – where Facebook does not operate mandatory transparency requirements – is another insightful example. In the Colombian 2019 regional elections, only four of the thirty-two successful regional governorate candidates availed themselves of Facebook's optional transparency tools for political ads. Out of the twenty-eight candidates who did not avail themselves of Facebook's optional transparency tools, twenty-two of them had a named Facebook account listed as a "public figure" or "politician" well before the 2019 elections.[14]

Google

In a select number of countries, Google applies mandatory verification checks for advertisers and displays ads in an online repository known as the Google Transparency Report. Currently, the countries where Google requires authorisation requirements are EU member states, the UK, India, Israel, New Zealand, Australia, Taiwan, and the United

12 PI, *Online political ads -a study of inequality on transparency standards*. Available at: https://privacyinternational.org/sites/default/files/2021-01/AdsTransparency_TOPUBLISH.pdf

13 PI, *Electoral advertising, big data and privacy in Peru*, 7 February 2020. Available at: https://privacyinternational.org/node/3365

14 PI, *Online political ads -a study of inequality on transparency standards*. Available at: https://privacyinternational.org/sites/default/files/2021-01/AdsTransparency_TOPUBLISH.pdf

States.[15] At the time of writing, Google has provided "Transparency Reports" only in respect of a subset of these countries.[16]

In most other countries, Google allows for political advertising to be featured on its platform without restriction. In some places, the combined absence of advertiser checks and ad repository is egregious.

PI partner InternetLab conducted research on political advertising on Google in the November 2020 Brazilian municipal elections. In Brazil, the Google search platform is the most visited website in the country.[17] However, Google does not regulate political ads in the country.

In the 2020 municipal elections, Brazil had over 500,000 city council candidates and 19,000 mayoral candidates in more than 5,570 Brazilian municipalities.[18] The sheer number of candidates no doubt resulted in a flurry of election ads on Google. However, given that Google does not regulate political ads in Brazil, no "political transparency report" is available. Thus, it is impossible for civil society to monitor, analyse or otherwise view all election ads posted on its platform. Further, while electoral regulation in Brazil requires political parties and candidates to report expenses related to online 'content boosting', it does not make available granular information about election ads to the general public. The absence of regulation by Google, combined with the administrative unworkability for any public entity to monitor each of these ads, results in significant transparency harms for democracy.

Opt-out vs opt-in of political ads : privacy by choice vs by default

Political ads can be a key vector for disinformation. For this reason, it is important that online users are given the option to decide whether they want to see political ads in the first place.

15 Google, Advertising Policies Help, *Update to Political Content policy* (October 2020) https://support.google.com/adspolicy/answer/10138882?hl=en&ref_topic=29265

16 At the time of writing, EU member states, UK, India, Israel, New Zealand, Israel and the United States.

17 Datareportal, *Digital 2020: Brazil*, 17 February 2020. Available at: https://datareportal.com/reports/digital-2020-brazil

18 Monica Yanakiew, "Brazil municipal elections to signal where country is headed", Al Jazeera, 15 November 2020. Available at: https://www.aljazeera.com/news/2020/11/15/brazil-municipal-elections-signal-where-country-headed

In a statement on January 2020, Facebook stated that they would increase user control over political ads by allowing users to see fewer political ads, starting with the US.[19] In June, this control was activated for US users ahead of the US election.[20] While Facebook's original announcement stated the expanded transparency features would "apply in all countries where we facilitate "Paid for by" disclaimers on ads", it is PI's understanding that the tool has so far only been made available in Brazil ahead of the November 2020 municipal elections.[21] Google does not provide this option to its users.

While PI celebrates the fact that users are given the option to effectively "opt out" of political ads, we believe that the ideal starting point would be for political ads to be displayed on an "opt-in" basis. Opting-out arrangements effectively make exposure to political ads the default rule, and place the burden on the user to disable unwanted advertising. During the short window where default settings apply, even users who decide to opt-out may inadvertently be exposed to political advertising propagating disinformation. In this regard, we note that Facebook has repeatedly stated that it will not fact-check political ads on its platform.[22]

Online platforms should implement "opt-in" mechanisms for political ads, which would promote privacy by default.

III. The role of domestic legal frameworks

In order to address the exploitation of data that in turn feeds disinformation, consideration is needed of human rights mechanisms, including those protecting the right to privacy, the right to freedom of expression, and the right to political participation.

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

19 Rob Leathern, "Expanded Transparency and More Controls for Political Ads", Facebook, 9 January 2020. Available at: https://about.fb.com/news/2020/01/political-ads/

20 Naomi Gleit, "Launching The Largest Voting Information Effort in US History", Facebook, 16 June 2020. Available at: https://about.fb.com/news/2020/06/voting-information-center/

21 Facebook, "Mais controle e transparência para anuncios sobre política no Brasil", 4 August 2020. Available at: https://about.fb.com/br/news/2020/08/mais-controle-e-transparencia-para-anuncios-sobre-politica-no-brasil/

22 New York Times, "Facebook Says it Won't Back Down From Allowing Lies in Political Ads", 4 September 2020. Available at: https://www.nytimes.com/2020/01/09/technology/facebook-political-ads-lies.html

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

around the world have now enacted data protection legislation of varying strengths. When considering the effectiveness of these laws, it is important that they are comprehensive in their application, with a resourced, independent regulator; and that political parties or groups are not permitted to 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. However, a recent comparative analysis of legal frameworks governing political micro-targeting in Canada, Brazil, France, Italy, Spain and the UK, conducted by the University of Edinburgh in collaboration with PI, revealed that there are considerable gaps in regulation of such practices in domestic legal frameworks.[24]

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 rules covering financing limits, transparency safeguards, oversight mechanisms, and the media. 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 have not been extended to the digital environment and only the voter, campaigners and platform know who has been targeted with which messages.[25]

IV. Regulatory challenges

Preserving freedom of expression while protecting anonymity

Notwithstanding the general call for transparency above, PI accepts that special arrangements must be made to protect the anonymity of advertisers at risk. In a 2020 recommendation, PI and a coalition of organisations called on the European Commission to issue guidelines for platforms to protect advertisers in a high risk

cornerstone of State privacy protection. See UN High Commissioner for Human Rights, *The right to privacy in the digital age*. Available at: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/39/29

24 PI, *Micro-targeting in political campaigns: A comparative analysis of legal frameworks*. Available at: https://privacyinternational.org/report/4364/micro-targeting-political-campaigns-comparative-analysis-legal-frameworks

25 PI Recommendations, *Challenging Data Exploitation in Political Campaigning*, https://privacyinternational.org/advocacy/3981/challenging-data-exploitation-political-campaigning-pi-recommendations

context, and make suggestions for a mechanism for advertisers to anonymise their identity on the basis of threats and risk.[26]

However, it is key that for any such mechanism to be subject to independent oversight, as it could otherwise be abused as a loophole by advertisers trying to hide their identity. Exemption applications should be carefully scrutinised according to a transparent set of criteria and information should be made publicly available on the number of exemptions requested and granted on an annual/quarterly basis.

Regulating ads transparency in online platforms

Where online platforms refuse to implement heightened transparency standards, the question whether domestic election or data protection regulators should take steps to enforce transparency logically follows.

In some instances, electoral regulation of political advertising can spur online platforms to introduce heightened transparency rules. However, it can also have the opposite effect. In Canada, Google banned political advertising ahead of the Canadian federal election in 2019 after legislation was passed which required online platforms to keep a registry of all political and partisan ads they directly or indirectly published. [27] The Canadian example is a powerful lesson that electoral regulation does not guarantee corresponding transparency action by online platforms.

Conversely, electoral regulation can fall short of ensuring the transparency of the full range of political ads by restrictively limiting the types of advertisers who are required to register.

For example, ahead of the 2020 local elections in Indonesia, Facebook introduced mandatory verification requirements for political advertisers, including requiring political advertisers to provide the relevant candidate or political party's registration number issued by the General Electoral Commission.[28] Because only political parties/candidates are required by law to register with the Electoral Commission, this

26 European Partnership for Democracy, *Universal Advertising Transparency by Default*. Available at: https://epd.eu/wp-content/uploads/2020/09/joint-call-for-universal-ads-transparency.pdf

27 Tom Cardoso, "Google to ban political ads ahead of federal election, citing new transparency rules", The Globe and Mail, 4 March 2019. Available at: https://www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new/

28 Facebook, Business Help Center, *Get Authorized to Run Ads About Social Issues, Elections or Politics*. Available at: https://www.facebook.com/business/help/208949576550051?id=288762101909005&country_select=ID

meant that Facebook did not apply heightened verification requirements to advertisers who sought to publish political ads but were neither candidates nor obviously affiliated to political parties. In other words, it was possible for third parties to post political ads without verification. As a result, these were not included in the Facebook ad repository. Our case-study revealed a political ad promoting a candidate in the 2020 regional elections published by an account belonging to a mainstream media channel on Instagram, which had not undergone mandatory authorisation to post political ads. We were able to find this ad in the Ad Library as an ad that ran without a disclaimer, e.g. had not labelled itself as political. Though this ad was eventually taken down, it reached over 1 million people.