The Centre for Democracy & Technology, Europe Office's response to the European Commission's Public Consultation on Political Advertising

March 2021

Introduction

The Centre for Democracy & Technology, Europe Office (CDTE) has read with interest the questionnaire provided as part of the European Commission's public consultation on political advertising. While it contains many relevant and pressing questions, CDTE would like to present its own view on online advertising in general, in a concise format separate to the survey. Below, you will find analysis and recommendations on online political advertising and online advertising more generally. This submission reflects and builds on our responses to the Commission's consultations on the Digital Services Act and on the European Democracy Action Plan.

1. The risks of overly broad definitions of political ads

The questionnaire builds upon the assumption that political ads can be easily defined and distinguished from other, non-political, ads. CDTE warns that attempting to strictly categorise ads as "political" or "non-political" could pose high risks for the fundamental rights of individuals and civil society organisations. For this reason, we recommend a focus on specific activities during the defined election period (see below). While campaign ads from candidates may be clearly political, online campaigns addressing issues such as sexual and reproductive health rights, education, climate change, and migration can be more difficult to categorise. Online ads are cost-effective ways for nonprofits and advocates to reach audiences and raise citizens' awareness on critical issues for the public debate (this is without prejudice to our concerns about targeted ads below). Distinctions that categorise all ads as either political and non-political are inevitably arbitrary and should be avoided. If such distinctions must be made, "political" ads should be defined narrowly to avoid chilling the speech of many organisations and individuals lacking the resources to utilise traditional media to speak about important issues.

1.1 Cross-border campaigns and online civic space

The European elections are unique in that they are the only elections in the world whereby States vote for representatives in a parliament with a legislative mandate across 27 jurisdictions. That constitutes the largest trans-national democratic electorate in the world (375 million eligible voters in 2009). Pan-European debate during elections is essential to the credibility of European democracy. It will be important, therefore, that any measures aimed at restricting cross-border campaigning and financing are clear and proportionate. The EU's Fundamental Rights Agency has called on EU Member States to exercise caution when drafting and implementing legislation in areas which potentially (directly or indirectly) affect civil

society space, including freedom of expression, assembly and association, to ensure that their legislation does not place disproportionate requirements on civil society organisations and does not have a discriminatory impact on them. They have also stated that, under EU free movement of capital rules, civil society organisations should be free to solicit, receive and use funds from international bodies, organisations or agencies — this implies cross-border funding[1]. Civil society can play a crucial role both in monitoring election integrity and in ensuring a robust and vibrant debate around issues in the campaign — including by countering misleading information about the elections and otherwise combatting disinformation. This role should be protected and not overly restricted in the context of regulation of online campaigning.

1.2 Recommendations on protecting civic space

- Avoid drawing what will inevitably be arbitrary distinctions between all ads such as categories like political and non-political ads;
- Ensure that any regulations of online campaigns comply with applicable EU and international law, and do not disproportionately restrict or hinder human rights advocacy including during election periods, such as for European Parliament elections;
- If a distinction must be drawn, consider instead, during an election period, to restrict limitations only to content that an online business has been paid to host and that expressly advocates for the election or defeat of a candidate or political party for public office;
- Avoid restrictions on content posted by individual users or other organic content, or on content voicing a position on policy issues, even if those issues are associated with a political platform or party;
- Refrain from creating a rule or definition specific to existing online content formats. Strive instead to be agnostic as to delivery methods; and
- Consider other exceptions, e.g., for media coverage or for paid ads below a minimum expenditure threshold.

2. Online advertising transparency

Even beyond election periods, ad transparency is an important tool to help protect the integrity of the online digital space. The Commission should consider a content-agnostic approach to ad transparency by seeking the same kind of disclosures from all online advertisers. Source and targeting information about ads helps users understand why they see the ads they see online, but requiring intermediaries to discern political from non-political ads will likely lead to both overbroad and underinclusive categorization. As we have seen in efforts to create political ad databases, attempts to draw these distinctions can have significant unintended consequences for news media, bookstores and civil society organisations.

[1] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-challenges-facing-civil-society_en.pdf

Users should be able to easily determine that they have been targeted by an ad. We recommend that disclosures for *all* ads should include information about the purchaser of the ad and the nature of any targeting criteria, including any additional targeting that happens via the platform's recommender systems. This baseline transparency approach would give people access to information about the sponsors and techniques, on political (and non-political) advertising online.

Beyond mandatory disclosures for all ads, further transparency could be necessary to facilitate the effective enforcement of national electoral laws during an election period. In order to avoid any of the unintended consequences (see above) in relation to labelling 'political' ads, any additional transparency requirements should focus on information specific to the election or defeat of a political candidate or political party during an election period. This could include, for example, the relevant candidate and their party affiliation (if any); the identity, nationality, and country of residence of a sponsor if they place ads in support of a candidate or political party; the total amount spent on the ad campaign; the specific election the ad is referring to (if any); and targeting information for the ad. The information released by individual services about their advertisements should be required to fit a specific format, so that these reports are interoperable and comparable. This would facilitate researchers' and journalists', etc. ability to aggregate subsets of information for studying particular issues.

Finally, it should be emphasized that ad transparency comes with tradeoffs. In general, identification of the source of the funding behind an ad is an important piece of information for users, to understand how specific content is reaching them, and for accountability of the speaker and advertising system. But mandating the disclosure of individuals' identities can also harm individual privacy and undermine people's willingness to promote their speech online, whether it is a political opinion or an advocacy message that places the speaker at risk of reprisal. Anonymity and pseudonymity protect privacy and individuals' safety (e.g. persecuted minorities, human rights defenders in countries with rule of law challenges). Stringent transparency measures for all paid messages could interfere with individuals' political speech and could undermine the election law goals of equalizing political influence, improving the quality of electoral debate, and ensuring competitive elections. The European Data Protection Supervisor has advised that insofar as possible, that content moderation should not involve processing of personal data[2]. Any personal data collected in the context of ad transparency should only concern the information necessary for this specific purpose. To help assuage this concern, the European Commission may wish to consider limiting disclosure of the advertisers' identity to those ads in excess of a defined financial threshold.

2.1 Recommendations on ad transparency

- Consider a content-agnostic approach to ad transparency by seeking the same kind of disclosures from all online advertisers;

[2] Opinion 1/2021, on the Proposal for a Digital Services Act.

- Disclosures for *all* ads should include information about the purchaser of the ad and the nature of any targeting criteria, including any additional targeting that happens via the platforms recommender systems.
- In the context of an election period, the Commission could consider mandatory disclosure of:
    - the candidate and their party affiliation (if any);
    - the identity, nationality and country of residence of the sponsor;
    - the total amount spent on the ad campaign;
    - the specific election the ad is referring to (if any);
    - and targeting information for the ad.
- Consider limiting disclosure of the advertisers' identity to those ads in excess of a defined financial threshold.

3. Platform Recommender/Algorithmic Systems

Another area that deserves attention is the role that platform recommender systems play in shaping people's access to information and amplifying or suppressing specific content. These are at play for all online ads. Online content hosts are increasingly turning to measures beyond a simple "take down/leave up" paradigm for content moderation, to include actions against content that limit the incentives for users to post such content (e.g., demonetization, removing comment features) and that limit the content's reach (e.g., downranking and deprioritizing content).

Moving beyond the "take down/leave up" paradigm can be beneficial to free expression, because it provides intermediaries with a more diverse array of tools they can use to mitigate abuse, without totally silencing a user's speech. However, the operation of content amplification and recommender systems on online services are typically opaque, leaving it unclear to users how a service is deciding what content to display, and whether their posts are being penalized for including "borderline" speech. In general, online services should provide more information to their users about the criteria their content promotion algorithms and recommended systems use to decide what content to display; services should also explain in what circumstances downranking (or "shadowbanning") may be used to restrict the circulation of a post.

Along with increasing transparency into the operation of ranking algorithms and recommender systems, digital services should also provide enhanced user control over the criteria and values that inform what these systems display to them. The availability of such user control tools can improve user satisfaction and trust in recommender systems, and may encourage users to think critically about the kinds of information they seek to encounter. For instance, users could opt to receive recommendations outside their ordinary consumption habits and/or view content in chronological order rather than curated.

User control tools are not a perfect solution to the challenges posed by algorithmic amplification of content: some warn that increasing user control can also harden people's filter bubbles and enable users to deliberately view extremist content. Much depends on how the user control tools are implemented and designed, and the baseline assumptions that the content promotion algorithm is optimized to achieve (e.g. that the amount of time a user spends on the service should be maximized). More empirical research (and access to data) is needed to study the effects of amplification algorithms, and interventions such as user control features, in practice.

CDTE notes that oversight and auditing of algorithms has been tabled as part of the draft Digital Services Act. Ensuring robust, impartial and independent oversight of algorithms will require careful consideration and the development of new practices. CDTE is concerned that the proposed governance structure of the DSA lacks the requisite independence and competencies to carry out this role.

3.1 Recommendations on algorithms and recommender systems:

- Increase transparency into the operation of intermediaries' ranking algorithms and recommender systems;
- Provide enhanced user control over the criteria and values that inform what these systems display to them.

4. Micro-targeting and general targeting in the context of elections

Since the Facebook–Cambridge Analytica data breach occurred in 2018, there has been increased awareness of the challenges that online advertising pose to our democracies. Most EU Member States' electoral laws are designed for an era when political campaigning exclusively took place via door-to-door canvassing, postering and televised adverts and debates. The reality now is that the majority of voters use social media as the primary channel to seek information and get news. Political parties now spend more on online campaigns than on traditional campaigns. Although the cultural and political context (and therefore the electoral laws) differ across EU Member States, below we outline some safeguards which underscore the principles of fairness in political campaigning which would be worth further and careful consideration in the context of electoral integrity online.

4.1 Equal suffrage

This principle (See the Council of Europe's handbook for civil society organisations on using international election standards) includes the obligation for the state to be impartial towards candidates and parties. It applies in particular to electoral campaigns, coverage by the media (especially publicly owned media) and to public funding of parties and campaigns. It also means

states should prevent undue media dominance or concentration by privately controlled media groups in monopolistic situations that may be harmful to a diversity of sources and views.

In practice, at the national level there are often rules on how much time any political party or candidate can have on national airways or caps on the amount that can be spent on poster campaigns overall. Such rules generally do not exist yet for spending on online advertising. This opens the possibility to flood social media platforms with advertisements in support of one party or candidate. Member States should clarify how their offline national laws apply online.

4.2 Free suffrage

Free suffrage means free formation of voters' opinion and the free expression of this opinion. (See also the UN Human Rights Committee, General Comment 34, 2011). When considering whether this principle is being respected, we examine whether freedom of expression and freedom of political debate are respected. A challenge which arises in relation to this principle and online advertising is the use of personal data or demographic data to micro-target individual voters. Micro-targeting can be used (by advertisers or by ad systems, see Panoptykon Foundation's report 'Who (really) targets you?') to send tailored messages to specific groups, in ways that may serve to only reinforce pre-existing views and limit exposure to contrary opinions. State-sponsored interference campaigns have also used micro-targeting to reach specific groups with inflammatory messages.

Micro-targeting of political messages also raises questions of explicit consent and whether voters are aware that certain data about them is being used for this purpose. In a number of EU Member States, there are already safeguards to limit the range of demographic or other information which is permitted for use in traditional campaigns. A more robust enforcement of GDPR is desirable, as well as a deeper reflection at the national level with regard to what legitimate public-interest targeting might look like, i.e., use of non-identifiable cookie data to ensure that relevant election information hits the relevant geographic constituency.

4.3 Universal suffrage

Universal suffrage gives the right to vote to all adult citizens, regardless of wealth, income, gender, social status, race, ethnicity, or any other restriction, subject only to relatively minor exceptions. Voter suppression concerns allegations about various efforts, legal and illegal, used to prevent or discourage eligible voters from exercising their right to vote. Minorities and communities of color are unfortunately a typical target of this particular technique. With the use of personal and demographic data it is possible to run a campaign providing false information on election procedures or dissuading a targeted group from exercising their right to vote. In this instance again, transparency on the origin of such advertisements and limitations on how and what data can be used to target individuals will be important. The discriminatory impact of platforms' own recommender systems should also be considered.

4.4 GDPR and targeted advertising

There should also be more clarity on what informed and explicit consent means in the context of targeted advertising. According to the UK ICO's report, the Real Time Bidding (RTB) process may involve the processing of special categories of data such as political or religious affiliation, ethnicity, and mental or physical health. The GDPR expressly prohibits processing such information unless a condition within Art. 9 applies. The only applicable exception is in a case where explicit consent, as set out in Art. 9.2.a, has been given. Furthermore, in line with the GDPR Art. 35.3.a, online platforms involved in the RTB process are obliged to publish a data protection impact assessment (DPIA) before beginning the related personal data processing operations and to consult the competent Data Protection Authority if high risks remain following the DPIA.

In the case of behavioral advertising based on internet traffic, consumer control means, in line with GDPR Art. 7, that even after consumers have opted in to the data collection, it must be as easy to revoke as to give consent. Upon revocation, behavioral advertising networks and their ISP partners should stop using any data collected while the consumers were opted in. Otherwise, processing previously collected Internet traffic content data should be based on legal grounds other than consent and the consumers should be informed at the time when they revoke their consent.

4.5 Recommendations on targeted advertising:

- Compel EU Member States to ensure that there is clarity about how their offline electoral laws apply online, including limitations on spending, targeting and media blackouts;
- Recall that a minimum amount of targeting can be necessary to ensure that users have access to the relevant information in the context of an election; this can be done by using limited types of data, e.g., the language of the user's web browser and/or approximate location to determine their nationality/country of residence;
- Ensure broad transparency of all adverts and targeting methods in order to enable national watchdogs such as public authorities mandated to uphold electoral law, civil society and journalists as well as academic researchers to help monitor and enforce electoral safeguards irrespective of the national differences in approach;
- A more robust enforcement of the GDPR:
    - in line with the GDPR 'privacy by default' principle, third party cookies should be blocked by default in every web browser (e.g., Tor, Brave, Safari, Firefox, DuckDuckgo, Chrome, Opera);
    - in line with the GDPR storage limitation principle, non-essential cookie data should be dropped at the end of each session by default in every web browser (e.g., Firefox ETP 2.0);
    - in line with the GDPR data minimisation principle, cookies should be designed to authenticate a user without using direct identifiers (e.g., Trust Tokens);

- in accordance with the requirements of data protection by design and by default that recommender systems should not be based on ‘profiling’ in line with Art. 4 (4) of GDPR (see also the Opinion of the EDPS on the DSA).