CENTER FOR
DEMOCRACY
& TECHNOLOGY

Center for Democracy & Technology's Response to the European Commission's Public survey for European Democracy Action plan

I. Questions on election integrity and political advertising

1. Transparency of political advertising

Question 3:
To what extent do you agree with the following statements related to targeted political content you have seen online?

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know/No reply
1. Targeted content was labelled in a clear manner		X				
2. It was easy to distinguish paid for targeted content from organic content		X				
3. It was easy to identify the party or the candidate behind the content				X		
4. The content included information on who paid for it			X			
5. The information provided with the content included targeting criteria		X				

6. The ad was linked to a database of targeted political content		X				
7. The targeted political content offered the possibility to report it to the platform		X				

Question 4:
Which of the following initiatives/actions would be important for you as a target of political content?

	Not at all	A little	Neither a lot nor a little	A lot	Absolutely	Don't know
1. Disclosure rules (transparency on the origin of political content)					X	
2. Limitation of micro-targeting of political content, including based on sensitive criteria, and in respect of data protection rules					X	
3. Creation of open and transparent political advertisements archives and registries that show all the targeted political content, as well as data on who paid for it and how much					X	
4. Political parties to disclose their campaign					X	

finances broken down by media outlet						
5. Prohibit foreign online targeted political content						
6. Prohibit online targeted political content altogether						
7. Rules limiting targeted political content on the election day and just before						
8. Other						

Question 5:
Online targeted political content may make use of micro-targeting techniques allowing advertisers to target with high precision people living in a specific location, of a certain age, ethnicity, sexual orientation or with very specific interests. Do you think that:

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree	I don't know /No reply
1. Micro-targeting is acceptable for online political content and it should not be limited				X		
2. Criteria for micro-targeting of political content should be publicly disclosed in a clear and transparent way for every ad	X					

3. Micro-targeting criteria should be strictly limited	X					
4. Micro-targeting criteria should be banned				X		

Please explain:

CDT sees a number of significant risks to defining ‘political ads’ and rather advocates for the same transparency measures on all ads (see our DSA submission). Nevertheless this question raises significant points in relation to equality which merit attention; these points should be considered in relation to all online ads.

The question mentions age, ethnicity, sexual orientation. In fact, EU law covers any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation (the Equality Directives). Whilst there are limitations in EU law on the application of anti-discrimination provisions to online ads (see EU Directive on implementing the principle of equal treatment between men and women in access to and the supply of goods and services Directive 2004/113/EC), we should separate this from the impact of discrimination for targeted and data driven ads. For example, we know that techniques such as voter suppression (see below) or algorithm driven ad campaigns can disproportionately harm groups at-risk to discrimination. It should be considered how EU anti-discrimination safeguards can be upheld and enforced in the online campaigning context.

Ethnicity and sexual orientation are also aspects covered as special categories of personal data under GDPR Art.9. Targeting anyone upon these characteristics is already prohibited by EU law unless explicit consent is attained (see our DSA response for further clarification). There should be more clarity on what informed and explicit consent mean under GDPR in this case. Transparency on this point is also vital to allow individuals to contest the basis on which they are targeted.

The Commission should exercise great caution if it decides to define “political” ads.

Furthermore, we want to remind the Commission that attempting to distinguish “political” from “non-political” ads could pose high risks for the fundamental rights of individuals and civil society organisations. While campaign ads from candidates may be clearly political, messages addressing issues such as abortion, education, climate change, and immigration can be difficult to categorize. Online ads are cost-effective ways for nonprofits and advocates to reach audiences and raise citizens' awareness on critical issues for the public debate. An overbroad definition of "political" ads would chill the speech of many organizations lacking the resources to utilise traditional media. A narrow definition could reduce the Commission's ability to address certain aspects of political influence online, but it would also reduce the negative consequences for free expression. If further restrictions were considered, for example during an election period, such measures should apply only to content that an online business has been paid to host, that expressly advocates for the election or defeat of a candidate or political party for public office. It should not apply to content posted by individual users or other organic content, or to content voicing a position on policy issues, even if those issues are associated with a political platform or party. The Commission should be wary of creating a rule or definition specific to existing online content formats. It should strive to be agnostic as to delivery methods and should consider other exceptions, e.g. for media coverage or for paid ads below a minimum expenditure threshold.

2. Threats to electoral integrity

Question 1:
Do you believe the following are real and existing threats to the electoral process in the EU and its Member States?

	Yes	No	Don't know
1. Intimidation of minorities	X		
2. Intimidation of political opposition	X		
3. Micro-targeting of political messages, that is messages targeted to you or a narrowly defined group	X		
4. Information suppression, that is the purposeful lack of information on a topic	X		
5. Disinformation or fake accounts run by governments, including foreign governments	X		
6. Divisive content, that is content created to divide society on an issue			

7. The amplification of content that makes it difficult for you to encounter differing voices	X		
8. Intimidation of women candidates	X		
9. I or someone I know has been targeted based on sensitive criteria such as gender, ethnicity or sexual orientation	X		
10. Content where I could not easily determine whether it was an advertisement or a news post	X		
11. Other	X		

Please explain:

Since the Facebook–Cambridge Analytica data breach occurred in 2018, there has been increased awareness at the challenge that online advertising poses to our democracies. In that case millions of users' personal data was harvested without consent by Cambridge Analytica to be predominantly used for political advertising. Most EU Member States' electoral laws are designed for an era where 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 are increasingly spending more on online campaigns than on traditional campaigns. Although the cultural and political context and therefore the electoral laws differ across EU member states, there are 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.

Equal suffrage

This principle (See Council of Europe 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 national level there are often rules on how much time any political party or candidate can have on national airways or else 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. In our Digital Services Act submission, we have outlined the importance of transparency of all adverts in order to enable 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.

Free suffrage

Free suffrage means free formation of voters' opinion and the free expression of this opinion. 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 in 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, **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 the GDPR would be important in this regard, as well as further reflection on the need to provide regular information and options to users about the grounds upon which they are being targeted.

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 eligible voters from exercising their right to vote. Minorities are unfortunately a typical target of this phenomenon. 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.

3. European Political Parties:

Question 1:

Is there scope to further give a stronger European component to the future campaigns for EU elections? Please list initiatives important to you in this regard:

Other

Please explain:

The European elections are unique in that it is the only election in the world whereby States vote for representatives in a parliament with a legislative mandate across 27 jurisdictions. It is therefore 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 financing and campaigning are clear and proportionate. In the most recent European Elections, for example, concern was raised about a number of pan-European civil society campaigns which were blocked due to restrictions on 'foreign interference'. The European Commission should 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.

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.

4. European Elections

Question 1:
In your opinion, what initiatives at national level could strengthen monitoring and enforcement of electoral rules and support the integrity of European elections (multiple selections possible)?

- Clear rules for delivery of political ads online in electoral periods, similarly to those that exist in traditional media (TV, radio and press)
- Enhanced reporting obligations (e.g. to national electoral management bodies) on advertisers in a campaign period

- Enhanced transparency of measures taken by online platforms in the context of elections, as well as meaningful transparency of algorithmic systems involved in the recommendation of content
- Privacy-compliant access to platform data for researchers to better understand the impact of the online advertisement ecosystem on the integrity of democratic processes

Please explain:

As explained in question 5, attempting to distinguish “political” from “non-political” ads could pose high risks for the fundamental rights of individuals and civil society organisations.

As an alternative, the Commission should consider a content-agnostic approach to ad transparency by seeking the same kind of disclosures from all online advertisers. If the Commission requires disclosures in any form, it should also establish a centralized, open access, machine-readable database for the disclosed information. Through this database, electoral commissions, researchers and civil society organizations could analyze and identify trends in advertising, such as targeting efforts, uses of sensitive criteria, or discriminatory outcomes. This research could encourage voluntary efforts to address problematic practices and inform further regulatory approaches. 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, civil society organizations, and other non-political speakers.

The Commission should exercise great caution if it decides to define “political” ads (please see our explanation to question 5 for further analysis).

II. Questions on tackling disinformation

4. Enhancing users' awareness

Question 1:
Do you agree that the following kinds of measures would help enhance user’s awareness about how platforms operate and prioritise what users see first?

	Fully agree	Somewhat agree	Neither agree not disagree	Somewhat disagree	Fully disagree
1. Promoting content from trustworthy sources		X			
2. Promoting factual content from public authorities (e.g. on election date)		X			
3. Providing tools to users to flag false or misleading content	X				
4. Demoting content fact-checked as false or misleading		X			
5. Labelling content fact-checked as false or misleading without demoting		X			
6. Platforms should inform users that have been exposed to fact-checked content	X				
7. Removing content which is found false or misleading and contrary to terms of service (e.g. threatening health or public safety)			X		

Question 2:
In your opinion, to what extent, if at all, can the following measures reduce the spread of disinformation?

Other

Please explain:

Some of the above mentioned options have the potential to have a positive impact on tackling disinformation, and further research is required to understand their real effects. One area that deserves particular attention is the use of “downranking” or “shadowbanning” as a part of content moderation on a service. 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). Such responses can be beneficial to free expression, because they avoid a total silencing of speech that does not actually violate the service’s content policy, while also being effective at mitigating abuse. But when the operation of algorithmic systems is generally opaque, the potential use of downranking creates an environment ripe for confusion and conspiracy theories about exactly how a service is or is not manipulating content. Moreover, if demotion of a specific piece of content follows a failed fact-check by a journalist or a fact-checking organization, there needs to be proper safeguards for the independence and trustworthiness of the fact-checking entity and the process.

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. Providing user control requires recommender systems to be more transparent and explainable. This can encourage users to look beyond their known interests and generally improve user satisfaction and trust. For instance, users could opt to receive recommendations outside their ordinary consumption habits and/or view content in chronological order rather than curated. Some would warn that increasing user control can also enable users to deliberately view extremist or contentious content. Much depends on how the tool is implemented and designed, and more empirical research (and access to data) is needed to study its effects in practice.”

Companies are also encouraged to run notice-and-action (N&A) systems where users can flag content as violating the service’s own policies. For instance, Facebook allows users to report content they consider to be 'false news'. If their report is approved, Facebook significantly reduces the distribution of the content at issue and shows it lower in the News Feed. As there is usually a fine line between false news and satire or opinion, there also need to be proper safeguards including the right of the content uploader to issue a counter-notice. The details on accountable and transparent content moderation practices (including N&A systems) can be found in the Santa Clara Principles, which CDT helped to craft in 2018. It should be reiterated that reports of false news or disinformation need to be kept clearly distinct from reports of content deemed to be illegal, where different logic and procedures apply (please see our response to the public consultation on the Digital Services Act for more information).

Question 3:
To what extent, if at all, do you support the following measures to reduce the spread of disinformation?

Other

Please explain:

See answer above

What safeguards and redress mechanisms do you consider appropriate and necessary to avoid errors and protect users' rights?

In our DSA submission we have detailed the need for a harmonised, transparent, rights-protective notice-and-action framework. There should be avenues and procedural safeguards on remedy including the possibility to restore wrongfully removed content.

With respect to content moderation on platforms, neither human nor automated moderation processes are infallible—both can make mistakes. Service providers need to adequately train their moderation staff, and to test their automated systems, to ensure that the decisions reached by the human and machine portions of their moderation system reach the provider's intended outcome in almost every case.

Particular attention should be paid to automated tools used for content moderation, which are prone to error. Examples range from erroneous content takedowns, mass account suspensions, misinterpretations of copyright infringement, wrong language translations and more. Due to its technical limitations, the use of automated tools should not be mandated by law. We also caution that many of the above-mentioned interventions are implemented in partially or fully automated systems.

Various types of error in content moderation systems can be mitigated to a certain extent, by improving the quality of training for moderators and instituting regular processes for evaluating the results of the system. The element of human review remains a key component of any content moderation system. But error will never be entirely eliminated from content moderation—human communication is simply too complex and dynamic. Thus, it is imperative that any content moderation system includes a robust, transparent appeals process, including notifications to users about the reasons that their content has been removed or their accounts deactivated, and the opportunity to provide explanations or additional information. Any decisions on the legality of speech must remain the sole purview of the courts.

Question 6:
End-to-end encrypted messaging services (such as WhatsApp, Telegram or Signal) can be used to spread false and harmful content. In your view, should such platforms introduce measures to limit the spread of disinformation, with full respect of encryption and data protection law (more than one reply is possible)?

Other

Please explain:

Encryption is crucial for protecting personal communications and keeping businesses and organizations secure. None of the above mentioned measures should be implemented if doing so requires providers to weaken the encryption on their services.

Companies have already introduced features into their services with the aim to tackle the spread of disinformation which ensures that these services remain both encrypted and secure. For instance, Whatsapp has recently implemented a new feature into its system that allows users to fact-check the contents of viral messages. This new function does not require the WhatsApp server to decrypt messages, and instead gives users the choice to upload message content to Google to verify the content they receive. It comes in the form of a magnifying glass icon that appears next to messages that have been forwarded through chains of five or more people. Tapping it performs a Google search of the message's contents, with the aim of revealing whether it contains conspiracy theories, fake news, or misinformation. The company has also introduced limits on the forwarding of messages. Until 2018, users had been able to forward a message to groups of 250 people at a time. That number was reduced to 20 that year, to five in 2019, and this year, to just one. These measures, however, cannot be unified and should not be mandated by law, as different services might have different characteristics, userbases, and serve different purposes.

Question 9:
Which information should online platforms publish about their factchecking/content moderation policy?

	Yes	No	Don't know
1. If they pay directly the factcheckers or if they work with an external factchecking organisation	X		
2. How they decide which posts are factchecked	X		
3. How many posts are factchecked	X		
4. How to flag posts to be factchecked	X		
5. Other, (please specify)	X		

Please explain:

Based on CDT's years of experience researching and advocating for increased transparency from Internet companies, we offer the following recommendations:

- Transparency for a purpose, not just transparency's sake. Transparency is not an end goal in itself; rather, information from online service providers should enable concrete policy goals such as accountability of companies and governments over actions they take against user content, and increased user control over the information they share and receive online. Any effort around transparency should have a clearly identified set of goals that the transparency measures are directly designed to advance.

- Transparency efforts need to be tailored to specific audiences. The umbrella concept of "transparency" can encompass many things, from detailed data about actions taken against user content and accounts, to information about policies and practices, to independent evaluations of a provider's systems. Different audiences will benefit from different types of information:

    - For users, CDT recommends that online services provide clear and detailed information about their policies, illustrated with examples to help users understand where the service draws lines between permissible and prohibited speech. This should include clear information about how content is algorithmically targeted and promoted on the site, as well as information about when and by whom any fact-checking label is applied. Services should provide clear information about the ability to report content, the opportunity to appeal actions taken against content, and the tools available to users to control the use of their personal data and the targeting or recommendation of information that they see on the service. The overarching goal of transparency aimed at users should be to empower users to make choices and exert control over their interaction with the service.

    - For independent research, services should make data available in structured, machine-readable formats. There are genuine privacy concerns associated with, for example, making detailed data about individuals' social media usage available to researchers; privacy and security controls over data made available to third-parties should align with the sensitivity of the information disclosed. For example, some data should be available in open-access formats, such as databases of advertising content and targeting information or information about public posts that have been labeled as false or misleading by a fact-checker. Generally, information that has been publicly available on a service should be made accessible in formats that enable independent research. More sensitive data, including information about non-public activity on a service, should only be provided to vetted researchers.

- Transparency reporting will look different across different services. Content moderation necessarily represents a series of trade-offs, and different services will (and should) experiment with different approaches to responding to the specific types of abuse that are most prevalent or problematic on their services. Extremely prescriptive requirements for the content and format of transparency reports could have the unintended consequence of constraining the ability of services to respond effectively to abusive content. For example, requiring services to report the length of time it takes to respond to notifications will exert a strong pressure on services to shorten that time, which will likely decrease the quality of the review that they conduct. Any framework for transparency reporting needs to be flexible and to account for necessary variation in content moderation across services.

For more information, please contact:

Emma Llansó, Director, Free Expression Project, ellanso@cdt.org

David Nosák, European Affairs Associate, dnosak@cdt.org

Pasquale Esposito, European Affairs Associate, pesposito@cdt.org