CIVIL LIBERTIES UNION FOR EUROPE

SOLUTIONS FOR REGULATING MICROTARGETED POLITICAL ADVERTISING

By Éva Simon • Advocacy Officer • Civil Liberties Union for Europe

December 2020

Table of contents

Solutions for Regulating Microtargeted Political Advertising

Article 2 of the Treaty on European Union states that democracy is one of the EU's founding values. A properly functioning democracy relies on EU residents being able to have access to reliable information, freely form opinions and express their views in political debates. The potential to influence people over political issues has never been greater. This is because online platforms easily allow political organisations to pay to promote personalised messages towards individuals fitting certain targeting criteria.

Social media platforms curate content for users. Platforms offer each individual different content depending on the prediction of an algorithm: what will catch or retain their interest. In addition to this, individuals and organisations can pay to promote content to users who fit certain criteria. The elements of content curation, paid-for promotion of content, and microtargeting combine to produce filter bubbles and echo chambers. These terms refer to online spaces where individuals receive information specifically targeted to them that conform to and reinforce their own beliefs, mainly caused by the personalization of social media platforms. In this way, microtargeting allows political parties to say different things to different people, preventing a proper public debate on political agendas. They can also promote misleading messages aimed at manipulating voters, including actively discouraging voters from even voting at all.

The issue of microtargeted political advertising[1] has been at the heart of the debate over elections for years now, with more intensity since 2018, following the Cambridge Analytica[2] scandal. Investigations into Cambridge Analytica revealed that distorted and targeted messages can manipulate people's opinions without their knowledge. European decision-makers have been looking for solutions[3] to avoid malign actors compromising fair elections, distorting political debates, influencing voters, and feeding them with biased information.

There is already common acceptance among stakeholders, including online platforms[4], that greater transparency will contribute towards preventing the damaging impacts of microtargeted political advertising. However, transparency is only a first step. Transparency rules need to be enforced, and further steps are needed to properly protect the fundamental rights of European voters, their freedom of expression, the right to access information, and their personal data protection.

In the present policy paper, we explain what measures European and national authorities should take beyond merely improving transparency. In particular, we argue that proper application of the General Data Protection Regulation (GDPR)[5] could safeguard EU residents' rights. Proper application of the GDPR would facilitate the realisation of the right to access to information, promote free

participation in public discussion, and also protect their personal data. GDPR enforcement is in the hands of national authorities and the European Commission; they can help stakeholders understand how to implement GDPR rules in relation to political advertisements.

Liberties advocates for the following solutions concerning targeted political messages:

1. Political parties and interest groups that use advertising, and online platforms that host this paid-for content, should be required to meet certain transparency requirements. In particular, they should be required to publish a wide range of data about political advertisements and what targeting methods are offered by them. This obligation should be mandatory for both platforms and interest groups.

2. Political parties, interest groups and platforms, in fulfilment of their transparency obligations, should be required to conduct and publish Data Protection Impact Assessments relating to online political campaigns hosted on relevant platforms. Data Protection Authorities (DPAs) have the authority to order binding remedial action. This includes issuing fines to online platforms and political parties or interest groups and referral of the DPA's findings to national electoral commissions. Joint liability of platforms and political parties could force them to follow the rules.

3. Political messages should have different limitations according to certain factors, such as whom the message is for, whether it is tailored and targeted to a homogenous group of people, and whether it has an immediate or recent political context. We have to differentiate between political messages that merely inform people about an election date, or messages from NGOs informing the public about public health rules during the COVID-19, and a tailored message to eldery men that tries to convince them to vote against abortion. These factors should be weighed on a case-by-case basis. This approach of weighing up relevant factors to detect political advertising means that authorities need not try to regulate the content of political advertising.

4. The Commission and national DPAs must properly enforce the GDPR. According to the GDPR, individuals may only be targeted on the basis of their personal data if the person opts-in to be targeted by political messages. The European Commission should elaborate guidance to clarify how the GDPR should be applied for political advertising.

5. Online platforms, political actors, and user organisations should cooperate and set clear agreements to help protect users' fundamental rights on online platforms and ensure vibrant and diverse political discourse. This could serve as a first step of a code of practice similar to the existing code on disinformation or the agreement on discriminatory advertising in the United States[6].

Why are targeted political messages problematic for the proper functioning of democratic debate?

There are two problems created by targeted political messages. First, they polarise and distort political discourse. They target people with messages that have been created to resonate with that person, on the basis of data collected online about that person's behaviour. Messages tailored to homogenous groups are offered by social media platforms so that advertisers target their messages towards people who meet certain criteria, and this delineates the groups. For example, political parties and social media platforms might determine that the demographic group of women between 25-35 living in urban areas with a university education share certain interests, concerns and opinions, even though the targeted group does not conceive itself as a distinct social group. A platform's choice of curated content for people in this group as well as targeted advertising results in a bubble where people are locked in an echo chamber. In this echo chamber, they receive opinions that reflect their supposed beliefs. In this group the chance to listen to and get access to a wide range of information, differing viewpoints, or participate in balanced political debates is less likely. When individuals only receive information tailored to them, this results in a limitation on access to information. This in turn makes it difficult to form an opinion based on consideration of different perspectives and sources of information. This leads to increased polarisation in society, and the lack of healthy public debate may also compromise the fairness of elections.

While this kind of microtargeting can polarise public opinion and distort public debate, there is a further compounding danger when malign actors exploit these bubbles to disseminate disinformation and influence the political decision-making process. Disinformation campaigns[7] are based on tailored messages to certain groups, determined by targeting criteria, who are susceptible to manipulation through misinformation.

The second problem with being able to target political messages to people meeting certain criteria, is that it allows advertisers to select recipients on the basis of their profiles. This can lead to damaging situations that may include, among other things, prejudices they have expressed previously. Targeted and tailored advertising can also be used to exclude certain groups from receiving advertisements. For example, advertisements about employment, housing or participation in elections could be hidden from people belonging to certain marginalised groups by using targeting criteria to exclude according to national minorities, location, gender, or age categories.[8]

Why is it important to intervene?

The integrity of elections, freedom of expression, and the freedom to access and disseminate information are all key to healthy democracies. It is not possible to have balanced and informed democratic debate without freedom

of expression, which involves freedom to access and disseminate information. To preserve these values, we need to protect people from being targeted, according to data gathered about their behaviour, with tailored messages to alter their voting preferences or attitudes.

Transparency by default and going beyond

There is a common understanding among EU-level policy-makers that increased transparency is part of the solution to countering the damaging impact of targeted political messages. Online platforms, especially social media platforms, should be transparent about advertising rules so that both users and advertisers can understand what types of advertising method they use, and under which conditions. Full transparency would also allow better identification and understanding of malign actors. On the other hand, those doing the targeting, such as political parties and other political actors, should also be transparent about their spending and the messages they deliver to the public. Political parties are supposed to set out their agendas to the general public consistently. This allows citizens, journalists and others to have an open debate and discuss different viewpoints in order to evaluate and challenge those political agendas. But targeted advertising allows a political actor to give potentially conflicting agendas that aren't debated or open to discussion from opposing viewpoints, because they're delivered to people in a bubble who all have similar opinions.

Targeting and tailoring messages creates filter bubbles that alter the information ecosystems and influence political decisions and election outcomes. Therefore, transparency must be one of the basic principles of any regulation regarding targeted political messages. Platforms and political advertisers should also publish data at least once a year, in a structured data file available in an easy-to-access, easy-to-understand way, with regular updates. This will allow legislators, regulatory bodies and researchers to understand the impact, and elaborate proper regulations.

Transparency is necessary yet insufficient to solve the problems related to targeted political advertisements. As a first step, transparency rules must be enforced, but transparency by itself is far from enough to properly protect the fundamental rights of European citizens, their freedom of expression, the right to access information, and the protection of their personal data protection. Transparency helps authorities, users, and other interested stakeholders learn about political advertising activities through information disclosed by political actors and platforms.

Making relevant data available would also help authorities and lawmakers to introduce measures to protect well-informed and balanced public debate. Such data would allow regulators to identify patterns such as large amounts of fundings from particular sources, or identify links between organisations and political parties, to identify concerted efforts to mislead public opinion and will help authorities develop measures to prevent these acts and mitigate their damaging impact. But we

need further safeguards to protect democratic debate and the fairness of elections.

Aside from introducing and enforcing transparency requirements, platforms and advertisers are obliged to use the data gathered to carry out Data Protection Impact Assessments. Analyzing the impact of targeted political campaigns and disclosing related data would serve as further safeguards to better protect fundamental rights.

For more elaborated analysis and recommendations concerning transparency, we refer readers to a joint paper published by the European Partnership for Democracy, to which Liberties contributed.[9] Liberties also endorses the findings of Ranking Digital Rights[10], and the research of Algorithm Watch[11].

Lack of definition of political advertisements and why it is not a problem

Any organisation, be it a political party or other interest group, can influence voters by targeting and tailoring messages. The problem is not that organisations use paid content to try to persuade people to support a particular cause. The problem is when promoted content is designed to distort political debate and democratic participation, either because it is deliberately misleading, because it is manipulative and duplicitous (by giving different messaging to different parts of the electorate), or because it discourages people from voting at all. These are worrisome trends regardless of the organisation behind them.

Solving these problems by defining 'political advertisements' and elaborating a content-based approach could seriously limit freedom of expression and freedom of information. Liberties believes that this is not necessary to define political advertising. Instead, we recommend the following steps aimed at preventing the harms caused by targeted political advertising:

1. Transparency for regulatory purposes - so that regulators have a broad overview of which entities are targeting which messages towards which audiences, and the financial resources behind this.

2. Transparency for individual users - so that individuals know, when they see content, who is behind the advert, why they've been targeted, and based on what data.

3. Advertising standards - to prevent misinformation.

4. Proper application of the GDPR, which means that personal data in the online ecosystem can only be used for the purposes of delivering political advertisements if the user (data subject) asked for such targeted methods based on voluntarily shared data.

Targeted messages have some common features. These are issue-based messages reflecting the political sphere, aimed at influencing people to form political opinions. These messages

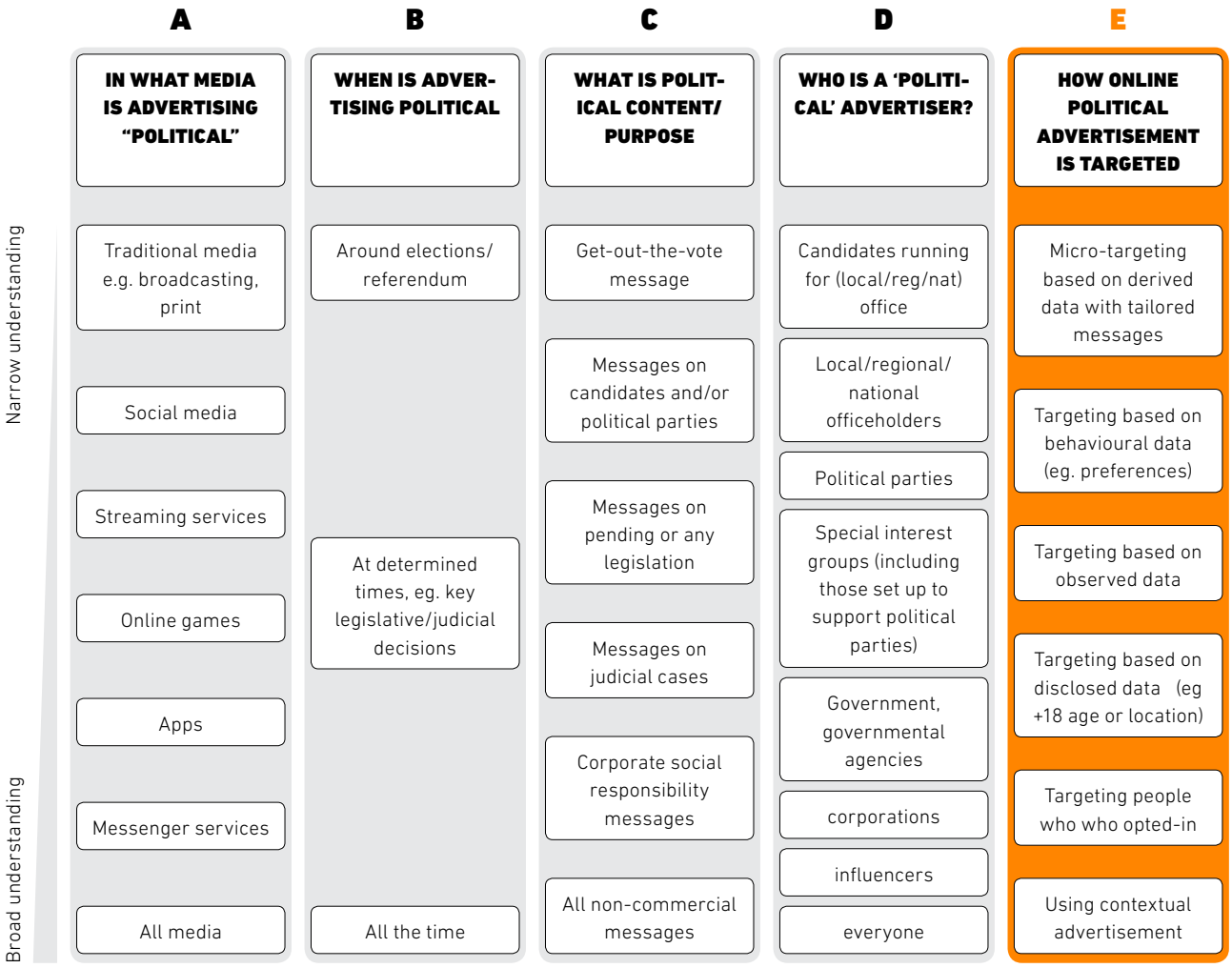
are delivered by targeting the users according to their behaviour[12] in the online ecosystem.[13]

Online platforms have already created categories for online political advertising. However, these definitions are often inconsistent with the requirements set out in the laws of EU Member States, and in many countries definitions do not even exist.[14]

Liberties is of the opinion that it is not necessary to create a common legal definition for political advertisements, because this is only required if authorities were to take a content regulation approach, which we discourage. First, content regulation is always very difficult and hardly ever used in legal regulation unless in very explicit cases, such as Holocaust denial. Second, an overly narrow or overly broad definition would create serious uncertainty in the field. Categorization of content has significant potential for overregulation and disproportionately limits freedom of expression recognised by the Charter of Fundamental Rights.

Instead of creating a definition for political speech, Liberties is of the opinion that regulators should determine whether to intervene based on an assessment of certain factors. Factor-based regulation is often used to regulate harmful content and illegal speech where context is an important consideration in distinguishing between legal and illegal speech. A common example is parody, which creates a certain legal context in most cases. We recommend that regulators make a determination as to whether to intervene by weighing certain criteria, which we set out below.

The following table was created by Paige Morrow from Article 19[15] and also used by Dr. Julian Jaursch in his paper Defining Online Political Advertising.[16] Liberties is of the opinion that an additional column is needed about the method of targeting. Important factors include consideration of the source of the personal data used, and whether it tries to influence homogenous groups of people. This table helps to understand the factors discussed above. The table offers guidance on a sliding scale. The closer that content is to the top of the table, the more likely a regulator should be to intervene, while the closer content is to the bottom of the table, the less likely a regulator should be to intervene.



Under the GDPR, it is unlawful to target people with political messages by default

The GDPR only allows limited targeting methods, requiring user consent even to limited data about them. By limiting the possibility of targeting mechanisms, we are protecting personal data and political speech at the same time. By setting fundamental rights-friendly requirements on how individuals and organisations can deliver political messages to the public, and limit microtargeting, this also supports the right to access information and protects free speech and free political debate.

Based on the GDPR, there are two legal bases[17] to process personal data of the users of an online platform in the targeting processes: either with the consent of the person, or for the purposes of a legitimate interest.[18]

Liberties is of the opinion that legitimate interest (GDPR Art 6 (1) (a) does not constitute a legal basis for targeting social media users with political messages. Social media

platforms should not consider their economic interests to be legitimate interests. Therefore, anyone who targets social media users should have the consent of those targeted by political messages (GDPR Article 6 (1) (f).[19] This means that GDPR requires data controllers to obtain opt-in consent from the user, and this requirement should be enforced by national DPAs and the European Commission.

In the case of these social media platforms, whose business model is based on data harvesting, they should also follow the rules of the GDPR and require consent from the user to use their personal data for targeting. This means that anyone who wishes to get tailored messages should sign up for this 'service' voluntarily, based on an informed decision.[20]

But even targeting those who choose to opt-in would only offer platforms and advertisers limited criteria for targeting messages. There are three main categories of data sets to be used for targeting. First, targeting individuals on the basis of data provided by them. Second, targeting individuals on the basis of observed data—what groups they join, or what pages they like on social media. Third, targeting individuals on the basis of derived data, that is, based on algorithm-derived data about their possible interests. Those who opt-in can only be targeted by the first data sets. The use of observed data and derived data is not allowed for targeting, even in opt-in cases, because these categories are not transparent and not controlled by the user and therefore runs contrary to the GDPR.

Does it constitute a problem for the publishers and the advertising industry?

Proper enforcement of the GDPR will have an impact on advertising industry practices and affect how political messages are delivered. However, it does not mean that the industry will collapse or people will not get access to information.

First, because political advertising is only a small segment of the advertising industry. Second, there are other methods to deliver messages that do not rely on data sets based on the behaviours of voters. In particular, there is great potential in contextual advertising. Contextual advertising respects the fundamental rights of the users because it is not relying on personal data. Contextual advertising is also a form of targeted advertising, but it relies on the keywords of the content visited by the user, and not his/her profile. Therefore, contextual advertising does not rely on cookies, tracking pixels, or profiling mechanisms of platforms, but on the page(s) the user visits.

The advertising industry claims that publisher revenues would decrease if content producers were forced to abandon targeting and tracking. However, in cases where providers switched from behavioural to contextual targeting, revenue grew. We only have limited data so far, but research conducted by Brave[21] shows that switching to contextual advertising does not mean revenue loss. The Netherlands' public broadcaster removed tracking cookies from their system and switched to contextual advertising and still grew ad revenue after

ditching trackers to target ads in the first half of 2020. It is noteworthy that this increase in revenue also occurred despite the coronavirus pandemic.

Less targeting also means great advantages to our democracies. Political parties would have to present themselves in the same way towards the public as a whole, which means political agendas are more likely to be properly debated, helping people consider different perspectives as they form their opinions.

How to regulate targeted political messages?

Targeted political messages based on the profiles of users created by platforms heavily rely on personal data. The GDPR sets clear rules against this. However, finding a solution is not easy, because targeting is widely used in all EU countries. As such, the political parties in the legislative branch that benefit from targeted campaigns have little incentive to limit their reach and influence.

Here we argue that the GDPR serves as a solid base for regulating the targeting methods of political messages. There are three main stakeholder groups in this chain (we do not consider agencies and other intermediaries as stakeholders in this paper):

1. The targeter, typically a political party or politician wishing to deliver information by targeting social media users;
2. Social media platforms, who collect and process data, create profiles, categories users, and directly interact with people;
3. The users or voters who are being targeted by political messages.

In this chain, social media platforms have a crucial role. They can provide proper safeguards to users to properly exercise their rights under the GDPR and offer business solutions to political parties, as targeters, at the same time. Prior consent to targeted messages can be delivered through platforms. It is important to repeat that consent should never be forced. Consent should fit the requirement of (Article 4 (11) and Article 7) of the GDPR—that it is freely given, specific, and informed.

If people wish to be subject to targeting, they can still opt-in for that purpose. This consent should be separated from accepting a platform's privacy policy or general terms of service. If consent is bundled up as a non-negotiable part of the terms and conditions, it is presumed not to have been freely given. Obtaining consent does not diminish the obligations of platforms or targeters to observe the data processing principles set out in Article 5 of the GDPR, such as fairness, necessity, or proportionality. Withdrawal of consent or any other objection could also go through the platforms.

Profiling and automation

We learned from investigations into Cambridge Analytica that obscure profiling

can seriously distort political debate and even election results. The creation of voter profiles is always based on data harvested by social media platforms. And this occurs through an automated decision-making process. Under Article 22 of the GDPR, everyone has the right not to be subject to these automated decision-making processes unless it is based on i) a contractual relationship; ii) authorised by law; or iii) it is based on the users' explicit consent. Points i) and ii) are not applicable in the case of social media services, even though they tend to argue to the contrary. This is because acceptance by a user of non-negotiable terms of service is not considered a contractual relationship. Therefore, data processing in relation to the automated decision-making process can only rely on users' explicit consent under Article 4 (11) of the GDPR. The right of the users to contest an automated decision entitles them not to consent to any kind of automated filtering method without human intervention. Users must be able to understand decisions made about them as well as understand how automated decision making affects them, and they must also understand how to contest a decision if necessary according to Article 21 (1) of the GDPR. Human intervention is also essential for transparent decision making and transparent appeal mechanisms to correct the imbalance between social media platforms and users. There cannot be an effective remedy without human intervention.

Suggestions

1. Political parties and interest groups that use advertising, and online platforms that host this paid-for content, should be required to meet certain transparency requirements. In particular, they should be required to publish a wide range of data about political advertisements and what targeting methods are offered by them. This obligation should be mandatory for both platforms and interest groups.

2. Political parties, interest groups and platforms, in fulfilment of their transparency obligations, should be required to conduct and publish Data Protection Impact Assessments relating to online political campaigns hosted on relevant platforms. Data Protection Authorities (DPAs) have the authority to order binding remedial action. This includes issuing fines to online platforms and political parties or interest groups and referral of the DPA's findings to national electoral commissions. Joint liability of platforms and political parties could force them to follow the rules.

3. Political messages should have different limitations according to certain factors, such as whom the message is for, whether it is tailored and targeted to a homogenous group of people, and whether it has an immediate or recent political context. We have to differentiate between political messages that merely inform people about an election date, or messages from NGOs informing the public about public health rules during the COVID-19, and a

tailored message to eldery men that tries to convince them to vote against abortion. These factors should be weighed on a case-by-case basis. This approach of weighing up relevant factors to detect political advertising means that authorities need not try to regulate the content of political advertising.

4. The Commission and national DPAs must properly enforce the GDPR. According to the GDPR, individuals may only be targeted on the basis of their personal data if the person opts-in to be targeted by political messages. The European Commission should elaborate guidance to clarify how the GDPR should be applied for political advertising.

5. Online platforms, political actors, and user organisations should cooperate and set clear agreements to help protect users' fundamental rights on online platforms and ensure vibrant and diverse political discourse. This could serve as a first step of a code of practice similar to the existing code on disinformation or the agreement on discriminatory advertising in the United States[22].

6. There are several other solutions that are worth thinking about. Who Targets Me lists five options[23] to intervene in order to shift the balance back to a more diverse political discourse. Among these solutions, "limitation on the number of campaigns that can be run" is an achievable solution. This would limit the number of simultaneous and distinct ads.

Notes

1 In this paper, we use the term targeted political messages or microtargeted political advertisements interchangeably. The reason is simple: we think that breaking down complex ideas helps to understand the problem.

2 Cambridge Analytica was a political consulting company involved in influencing the 2016 US elections, Brexit and so many others. CA harvested data without the knowledge or the permission of Facebook users and their contacts, to target them with political messaging and influence the outcomes of elections.

3 The Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee Report on the 2019 elections to the European Parliament, Brussels, 19.6.2020 COM(2020) 252 final.

4 In this paper we focus on social media platforms and refer to them as online platforms.

5 https://eur-lex.europa.eu/eli/reg/2016/679/oj

6 See footnote no. 8.

7 The most famous is the Macedonian fake news factory https://www.wired.com/2017/02/veles-macedonia-fake-news/

8 Targeting easily leads to discrimination based on age, gender, location, or any sensitive data. In spring 2019, a historic civil rights settlement was announced between Facebook, the American Civil Liberties Union, Outten & Golden LLP, and the Communications Workers of America. The settlement led to changes in Facebook's paid advertising platform to prevent discrimination in employment, housing, and credit advertising. Under the settlement, Facebook agreed to take proactive steps to prevent advertisers from engaging in unlawful discrimination when targeting users of Facebook, Instagram, and Messenger in relation to employment, housing, or credit. However, leading players of the American civil society and Facebook reached an agreement to protect fundamental rights. We believe that more is needed than ad hoc agreements.

9 https://epd.eu/2020/11/02/epd-joins-call-for-putting-meaningful-transparency-at-the-heart-of-the-digital-services-act/

10 Ranking Digital Rights produces the Corporate Accountability Index, which evaluates how transparent digital platforms and telecommunications companies are about policies and practices affecting freedom of expression and privacy, based on international human rights standards.

11 https://algorithmwatch.org/wp-content/uploads/2020/10/Governing-Platforms_DSA-Recommendations.pdf

12 Behavioural targeting is using information about the user's online behaviour to display advertisements. Retargeting is also a form of behavioural targeting, which uses information about users who already have shown interest in topics or products. We will use the term behavioural targeting both

referring to retargeting and original targeting methods.

13 It is important to distinguish between political messages and commercial advertisement. Not because they are using other targeting methods, but because of their impact on the society. Commercial advertisements are not the subject of this paper. It is also important to distinguish between targeting based on behaviour and contextual advertising. While the former has serious privacy implications, the latter properly fits the European data protection system.

14 Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation (ERGA Report), June 2019. https://erga-online.eu/wp-content/uploads/2019/06/ERGA-2019-06_Report-intermediate-monitoring-Code-of-Practice-on-disinformation.pdf

15 https://www.article19.org/

16 https://www.stiftung-nv.de/sites/default/files/snv_definingpoliticalads.pdf

17 Data subject's consent (Article 6(1)(a) GDPR) or legitimate interests (Article 6(1)(f) GDPR).

18 For detailed analysis see Guidelines 8/2020 on the targeting of social media users Version 1.0, adopted on 2 September 2020. However, we call attention to the significant difference between targeting political messages and other goods. While we can have a well-established argument that sanitary products are only targeted for a certain age group, we can not argue the same for political advertisements.

19 The Judgment in Fashion ID, 29 July 2019, C-40/17, para. 95 - ECLI:EU:C:2019:629, CJEU reiterated that in order for a processing to rely on the legitimate interest, three cumulative conditions should be met, namely (i) the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; (ii) the need to process personal data for the purposes of the legitimate interests pursued; and (iii) the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence. The CJEU also specified that in a situation of joint controllership "it is necessary that each of those controllers should pursue a legitimate interest […] through those processing operations in order for those operations to be justified in respect of each of them". https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf para 44. Liberties believes that in political campaigns, these cumulative conditions can never be met.

20 We call attention to the consent fatigue symptoms. https://www.beuc.eu/blog/e-privacy-and-the-doorstep-salesmen/.

21 Research can be found here: https://brave.com/publisher-3rd-party-tracking/

22 See footnote No. 8.

23 https://whotargets.me/en/what-to-do-about-microtargeting/

The Civil Liberties Union for Europe (Liberties) is a non-governmental organisation promoting and protecting the civil liberties of everyone in the European Union. We are headquartered in Berlin and have a presence in Brussels. Liberties is built on a network of national civil liberties NGOs from across the EU. Unless otherwise indicated, the opinions expressed by Liberties do not necessarily constitute the views of our member organisations.

Website:
liberties.eu

Contact info:
info@liberties.eu
The Civil Liberties Union for Europe e. V.
Ringbahnstr. 16-20
12099 Berlin
Germany

Please consider supporting Liberties:
https://www.liberties.eu/en/donate
IBAN: DE18 1009 0000 2679 5830 02
BIC: BEVODEBB (Berliner Volksbank)